THE UNIVERSITY of TEXAS SYSTEM
FOURTEEN INSTITUTIONS. UNLIMITED POSSIBILITIES.

UT DALLAS

Office of Internal Audit
800 W. Campbell Rd. SPN 32, Richardson, TX 75080
Phone 972-883-4876 Fax 972-883-6846

October 25, 2016

Dr. Richard Benson, President
Ms. Lisa Choate, Chair of the Institutional Audit Committee:

We have completed an audit of applications that are part of the TouchNet application suite as part of our fiscal year 2016 Audit Plan, and the report is attached for your review. The audit was conducted in accordance with the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*. The objective of our audit was to determine if adequate controls exist over the applications that are hosted by the TouchNet vendor.

Controls within the TouchNet application can be strengthened. The attached report details recommendations that will enhance the security and effectiveness of the TouchNet Application. Management has reviewed the recommendations and has provided responses and anticipated implementation dates. Though management is responsible for implementing the course of action outlined in the response, we will follow up on the status of implementation subsequent to the anticipated implementation dates. We appreciate the courtesies and considerations extended to us during our engagement. Please let me know if you have any questions or comments regarding this audit.

Toni Stephens
Institutional Chief Audit Executive

UT Dallas Responsible Parties
- *Budget & Finance*
  - Dr. Kim Laird, Associate Vice President and Controller
  - Dr. Reda Bernoussi, Associate Controller
  - Cheryl Friesenhahn, Director of Financial Services
  - Karol Miller, Treasury Manager
- *Office of Information Technology*
  - Frank Feagans, Associate Vice President of Enterprise Application Services & Director of Research
  - Jaideep Chitkara, Associate Director of EAS Shared Services
- *Office of Communications*
  - John Walls, Interim Vice President for Communications
  - Cary Delmark, Assistant Vice President Web Services

Members of the UT Dallas Institutional Audit Committee
- External Members
  - Mr. Bill Keffler
  - Mr. Ed Montgomery
  - Ms. Julie Knecht
- Dr. Hobson Wildenthal, Executive Vice President and Provost
- Dr. Calvin Jamison, Vice President for Administration
- Mr. Terry Pankratz, Vice President for Budget and Finance
- Mr. Brian Dourty, Interim Vice President and Chief Information Officer
- Dr. Bruce Gnade, Vice President for Research
- Dr. George Fair, Vice President for Diversity and Community Engagement; Compliance Officer
- Dr. Gene Fitch, Vice President for Student Affairs
- Dr. Inga Musselman, Senior Vice Provost
- Mr. Timothy Shaw, University Attorney

The University of Texas System
- System Audit Office

State of Texas Agencies
- Legislative Budget Board
- Governor's Office
- State Auditor's Office
- Sunset Advisory Commission

Executive Summary

TouchNet Application, Report No. 1703

Audit Objective and Scope: The objective of our audit was to determine if adequate controls exist over the applications that are hosted by the TouchNet vendor.

The following is a summary of the audit recommendations by risk level. See the Appendix for additional details.

Recommendation	Risk Level	Estimated Implementation Date
(1) *Centralize Responsibility for Application Security Administration*	**High**	June 30, 2017
(2) *Strengthen User Management Practices*	**High**	June 30, 2017
(3) *Enhance Governance of TouchNet Applications*	**Medium**	June 30, 2017

Responsible Vice Presidents:

- Terry Pankratz, Vice President for Budget and Finance
- Mr. Brian Dourty, Interim Vice President and Chief Information Officer (Recommendation 1 only)
- John Walls, Interim Vice President for Communications (Recommendation 2 only)

Responsible Parties:

Budget & Finance

- Dr. Kim Laird, Associate Vice President and Controller
- Dr. Reda Bernoussi, Associate Controller
- Cheryl Friesenhahn, Director of Financial Services
- Karol Miller, Treasury Manager

Office of Information Technology

- Frank Feagans, Associate Vice President of Enterprise Application Services & Director of Research (Recommendation 1 only)
- Jaideep Chitkara, Associate Director of EAS Shared Services (Recommendation 1 only)

Office of Communications

- Cary Delmark, Assistant Vice President Web Services (Recommendation 2 only)

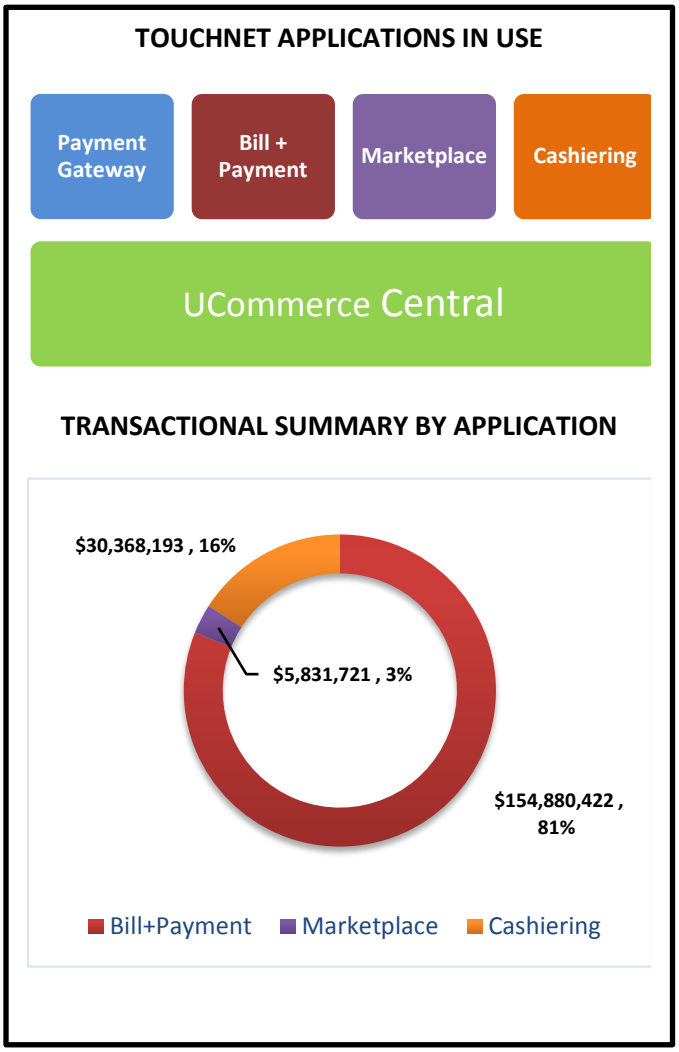
Staff Assigned to Audit:
Project Leader: Ali Subhani, CIA, CISA, GSNA, IT Audit Manager
Staff: Ray Khan, Staff Auditor.

Table of Contents

Background

Over the years, the importance of offering students the ability to make payments through credit and debit cards or directly route funds from their bank account to the university has greatly increased. Students now demand the convenience of electronic payments. As a result, higher education institutions now offer students the ability to initiate electronic transactions to pay for tuition and students fees, housing, parking and dining related costs. Additionally, departments at universities have also transitioned to ecommerce solutions that allow them to accept revenues for products and services online.

Implementation of electronic payment systems, however, can alter the risk profile significantly as institutions must better manage security and regulatory concerns. At UT Dallas, in order to better manage risks related to compliance with the Payment Card Industry (PCI), management outsourced hosting of the application suite in September 2014 to TouchNet, an outside vendor. Implementation of this application suite has allowed departments across the institution to efficiently and securely accept revenue. UT Dallas maintains responsibility for implementing application controls such as security administration and configuration within the applications.



The areas at UT Dallas responsible for administering the TouchNet applications include the Office of Budget and Finance and University Web Services. The Office of Information Technology has not historically administered the application; however, given the enterprise-wide impact of the application on the institution the audit report details a recommendation for IT to have more responsibility for security administration.

TouchNet currently offers the following application suite as part of the contract:

UCOMMERCE CENTRAL – This is the overall dashboard that provides integration between the different TouchNet applications.

PAYMENT GATEWAY – TouchNet Payment Gateway is the payment engine that assists in transferring campus payment transactions to financial institutions.

BILL+PAYMENT – provides students the functionality for online viewing of account balances, online bill presentment, and bill payments, as well as online access to payment plan set-up, enrollment, and installment payments.

MARKETPLACE – is the application where departments can create online stores and accept credit card payments for services or goods that may be offered within the department.

CASHIERING (Business Office) – integrates and centralizes in-person payments, point of sale payments, and departmental deposits with real-time support for both receivables and non-receivables. Currently UT Dallas has not fully rolled out the functionality for this application.

Audit Objective

The objective of our audit was to determine if adequate controls exist over the applications that are hosted by the TouchNet vendor.

Scope and Methodology

The scope of this audit was FY 2015 - 2016, and our fieldwork concluded on April 26, 2016[1]. To satisfy our objectives, we performed the following:

- Gaining an understanding of TouchNet applications and applicable processes.
- Reviewing policies and procedure documentation where available.
- Investigated the state of the user management within the various applications as well as how user security is being maintained and enforced.
- Determined if controls related to protection of sensitive data within the application are executing effectively and efficiently.
- Established if controls related to monitoring of user activities within the applications were in place.
- Ensured revenue from the Marketplace application consistently was posted to the Financial System.

Reconciliation of transactions between the Bill+Payment application and the Student system was not in scope for the current review but will be considered for a future audit. A separate audit of PCI compliance was conducted as part of the FY 2016 Audit Plan[2].

[1] Delay in report issuance was a result of waiting on management's responses and approvals to issue the report.
[2] http://www.utsystem.edu/sites/utsfiles/documents/system-audit/utd-pci-compliance-summary-memo/utd-pci-compliance-summary-memo.pdf

Where applicable, we conducted our examination in accordance with the guidelines set forth in The Institute of Internal Auditor's *International Standards for the Professional Practice of Internal Auditing*. The *Standards* set criteria for internal audit departments in the areas of independence, professional proficiency, scope and performance or audit work, and management of the internal auditing department.

Audit Results and Management's Responses

Controls
Our audit work indicated that the following controls currently exist:

- A formal agreement with the vendor who has responsibility for hosting the application exists.
- The Treasury department has a formalized process for getting stores set up within Marketplace.
- The Web Service department offers training to new storefront owners so that they can efficiently make use of the application.
- Revenue from the Marketplace application was being posted timely and accurately to the Financial System.

Audit Recommendations

Priority Findings – UT System - A UT System priority finding is defined by the UT System Audit Office as: "*an issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.*"[3] We have **no UT System Priority Findings** resulting from this audit.

However, although the above controls are in place, opportunities exist to enhance physical access controls as outlined below.

(1) Centralize Responsibility for Application Security Administration

Risk Level: **High**★

As noted earlier, the TouchNet vendor currently provides four separate applications/modules to enable the institution to carry out critical business functions. In addition, there is a central dashboard within the application suite that also provides limited reporting capability. The following departments have responsibility for administering security for each application:

[3] Appendix A defines the risks for all internal audit recommendations.

Application	Department Responsible for Security Administration
PAYMENT GATEWAY	Student Financial Services-Bursar
CASHIERING	Student Financial Services-Bursar
MARKETPLACE	Financial Management Services/Web Services
BILL+PAYMENT	Student Financial Services-Bursar

As a result of these responsibilities, a user must request access from separate departments if they require access to multiple applications that are developed by the TouchNet vendor. Additionally, this approach also does not provide adequate separation of duties, because administrative users are able to modify or approve one's own access privileges within the application without review. For example, a user with the role of User Administrator within TouchNet can assign themselves access to most of the other applications. This access would grant them the ability to view or make changes to information that is not required for their current role with the University.

Additionally, a Marketplace user with the Chief Administrator role could grant his or her own access to any role for any of the merchants. These access levels would allow the user to create discounts, issue refunds, and assign other individuals to these roles. Due to the limited logging within the application, any changes made would not be attributed to the user. According to the Information Security Office Account Management Standard [4], *"Access should be designed to maintain separation of duties to reduce the risk of a malicious individual performing conflicting activities (i.e. requesting system access while also approving one's own system access). Compensating controls such as log monitoring and system-enforced thresholds may also be implemented when conflicting duties cannot be separated."*

Recommendation: Management should consider centralizing the responsibility for application security with a department that regularly processes application security requests. In addition, the responsibility for administering the TouchNet applications should be transferred to the IT department since these applications are of strategic importance to the University's operations.

Management's Response: The Office of Budget and Finance will work with The Office of Information Technology to review existing roles and responsibilities with regard to administering TouchNet security. Appropriate alignment of responsibilities will be determined and executed to ensure proper segregation of duties.

Estimated Date of Implementation: *6/30/2017*

Person Responsible for Implementation: *Dr. Reda Bernoussi, Associate Controller; Frank Feagans,* Associate Vice President of Enterprise Application Services & Director of Research*; Jaideep Chitkara, Associate Director of EAS Shared Services*

[4] https://www.utdallas.edu/infosecurity/files/Account-Management-Standard.pdf

(2) Strengthen User Management Practices

Risk Level: **High**★

According to the Information Security Office Account Management Standard[5], "*Access privileges will be configured to not exceed the minimum necessary permission to perform job responsibilities*". During the review of access privileges that were currently set up within the applications, the following observations were made:

TouchNet Application Suite

- Access privileges requests are not being consistently documented or tracked in a tool. As a result, it is not possible to determine if adequate authorization exists for privileges that are currently assigned to individuals.
- With the exception of the Payment Gateway, all other TouchNet applications do not currently have logging that would indicate changes that are being made to user profiles and their associated security privileges. Subsequently, the ability to log other high risk activities was limited within certain applications.

U. Commerce Central

- 129 users were noted as being active within *U. Commerce Central* even though they were not currently affiliated with the university.
- 31 users were noted with the *User Administration* role assigned within the application even though they would not require such access privileges to carry out their job duties. The User Admin role provided the ability to create and modify users, adjust security privileges, reset user passwords, and modify the password policy that was enforced.
- Five users had the *U Commerce Central Administrator* role assigned within the application even though they would not require such access privileges to carry out their job duties. This role provides the ability to manage locations, users, roles and General Ledger codes that are currently set up in the application.

Bill Payment

- Eight users had the *TBP System Settings Administrator* role assigned within the application even though they would not require such access privileges to carry out their job responsibilities. The TBP System Settings Administrator role provides full access to all tasks and feature within the Bill+Payment application.
- One user was assigned the *Business Settings Administrator* role within the application even though they would not require such privileges to carry out their job responsibilities. This role provides access to all pages within the Bill Payment application but does not allow a user to change technical system settings.
- One user had the *eRefunds Manager* role within the application even though the user would not require such privileges to carry out their job responsibilities. This role allows users to perform all tasks related to refunds.

[5] https://www.utdallas.edu/infosecurity/files/Account-Management-Standard.pdf

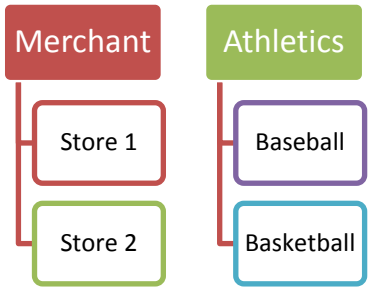
Payment Gateway

- Nine users were assigned the Administrator role within the application even though they would not require such privileges to carry out their job responsibilities. This role allows individuals to set up users and assign privileges within the application.

Marketplace

- Generic named administrator accounts were found. Such accounts reduce accountability as actions carried out under those accounts cannot be tied to one specific user.

- The Merchant Manager role provides elevated privileges, as it allows a user to assign store level access rights. We noted 161 users with the Merchant Manager role. As a result, any of these individuals would have the ability to assign users any role within their assigned merchant tree. Additionally, due to limited logging ability, any potential abuse of privileges would not be detected.



- The ability to create promotions within web stores is currently provided to all users assigned the role of Store and Merchant Manager. Due to reporting limitations within the application, we were unable to determine the specific number of users that are currently designated the Store Manager role. An individual with this access can directly set up store promotions, without any approvals or other mitigating controls. These promotions are customizable and can be created for single or multiple uses. Promotion codes can be generated in any denomination up to a maximum of a 100 percent value of the item/service that is being discounted.

  The Store Manager also has the ability to assign users any role within their assigned store tree. The current process could be abused, as there is no logging within the application that would indicate the specific user that created the promotion. According to the Financial Management Services department, individuals that are setup as Store Managers have responsibility for maintaining controls within the store and therefore would have accountability for all promotions that are setup. Currently, it does not appear that users with roles of Store and Merchant Manager receive training that would detail how to appropriately implement controls within their stores. As a result, individuals with responsibility for managing stores and merchants would not have an appropriate understanding of how to manage risks.

- Three users were noted with the *Chief Administrator* role within the application even though they would not require such privileges to carry out their job responsibilities. This role provides full access to all tasks and features within the Marketplace application and allows individuals to set up users and assign privileges within the application.

- Ten users had the *Administrator* role within the application even though they would not require such privileges to carry out their job responsibilities. One of these users is a student worker, while another user is no longer employed at the University. The Administrator role allows individuals to establish merchants and to assign privileges to the merchant users.

Recommendation: User access practices should be strengthened by:

a) Enhancing the checkout process so that privileges are terminated in a timely manner when they are no longer required.
b) Enhance the periodic security access review process to identify users that must have their privileges adjusted due to change.
c) Additionally, a process to consistently document privilege requests and the subsequent approval prior to adjusting privileges should be implemented.
d) Completing a comprehensive review of access privileges that are currently assigned within the TouchNet applications and limiting privileges to be in line with the user's job responsibilities.
e) Eliminating the use of shared generic administrator accounts.
f) Limiting the creation of promotions to Finance staff. Departments should be required to go through a documented approval to initiate the creation of promotions.
g) Determining if the vendor will enhance logging capabilities in the applications and consider alternatives if the vendor is unable to deliver an improved logging capability.
h) Enhance training that is already offered to users so that Store and Merchant managers have knowledge on controls that they have responsibility for implementing.

Management's Response:

a) Treasury will review users in the Marketplace application semi-annually and remove those users that no longer appear in the University's directory. A user will also be removed if it is determined that they are no longer affiliated with the assigned Marketplace storefront.

b) Treasury will develop additional measures to ensure that the Merchant Department Representatives notify Treasury when Marketplace users change responsibilities and no longer require Marketplace access.

c) *The Marketplace user roles are requested on the initial application. Treasury will work with Web Services to determine if enhancements can be made to the process for adding and updating users.*

d) *Review of access:*
   - *Treasury reviewed the user list provided by Audit. There were 8 users with the Chief Admin role and 7 with the Admin role. Four of the Admin users were removed and one Admin user's access was updated to correspond with their new role. All other users would maintain their roles in order to provide the appropriate services and assistance to the campus community.*
   - *The Bursar's department completed a review of access privileges for staff with the exception of Treasury staff that were currently assigned within U.Commerce Central and access privileges were adjusted to limit access to be in line with user's job responsibilities. The Bursar's department will be performing a semi-annual review in March and October to review individuals with access to the Bill Payment Suite and the Bursar's section of U.Commerce.*
   - *University Web Services reviewed 482 U.Commerce user accounts to determine which should have their privileges adjusted or revoked. From this review, 149 accounts were disabled for users who had never logged in, had not created a new account within the past six months, or were not found in the UT Dallas directory.*

e) *Administrator Roles:*
   - *The Administrator role is required by web developers in order to build and make requested changes to the various Marketplace storefronts. It is also required by Treasury staff in order to assist users and research transactions. The role is only provided to users who need it in order to manage the Marketplace application for the end users.*
   - *The number of Chief Administrator accounts was reduced from 13 to 9.*
   - *University Web Services has eliminated the use of shared administrator accounts. Shared administrator accounts were removed and more individual accounts were created to adjust for the removal of the Admin roles. We respectfully disagree with the finding that too many have the Administrator role. This role is required to build a storefront.*
   - *Only an administrator can create merchants and manage storefront development, including updating products and prices and providing technical assistance.*

f) *It is not practical for Financial Management Services to manage promotions for all Marketplace stores. The department managers are responsible for ensuring that processes are in place to ensure that all promotions are documented and properly used.*

g) Treasury will work with the vendor to determine what logging capabilities might be available.

h) Treasury will work with Web Services to determine what enhancements are needed for the Marketplace training module.

Estimated Date of Implementation: *6/30/2017*

Person Responsible for Implementation: *Dr. Reda Bernoussi, Associate Controller; Karol Miller, Treasury Manager; Cheryl Friesenhahn, Director of Financial Services; and Cary Delmark, Assistant Vice President Web Services*

(3) Enhance Governance of TouchNet Applications
Risk Level: **Medium**★

A strong governance framework allows institutions to effectively manage IT risks that are inherent with the implementation of a technology infrastructure. During the audit the following opportunities to enhance governance over the TouchNet Application Suite were noted:

- A reconciliation process between the payment gateway and the bank has not been historically performed. Such reconciliation would validate that revenue earned within Marketplace was accurately and timely received into the UTD bank account. Reconciliation was completed during the audit by Treasury staff that identified minor reconciling differences between Marketplace and the bank. However, due to the fact that the UTD bank statement does not detail the specific batch number for the Marketplace revenue that was deposited, Treasury is in the process of researching the cause of the difference.

- An overall policy and procedure manual that would adequately detail the critical processes and configurations that are in place currently does not exist. With the exception of the Bursar's office, we could not find any documentation of how critical processes relevant to the applications are carried out. Additionally, we could not find formal documentation detailing the responsibilities for each department relevant to the TouchNet application.

- Currently Web Stores within the Marketplace application that are no longer required are not being disabled in a timely manner.

Recommendation: Management should consider enhancing the governance framework related to the TouchNet applications by:

- Treasury must work with the vendor to identify the best strategy for tracking Marketplace revenue deposits into the bank.

- Developing a policy procedure manual that details all the critical processes and configurations for the applications. Additionally, formally designate individuals with responsibility for critical tasks.
- Disabling web stores in a timely manner once they are no longer in use.

Management's Response:

- *University Web Services reviewed 228 merchants to determine which should be adjusted due to change in status. The decision was based on a report of transactions from May through November, 2015. If the total amount collected by the merchant was zero, we disabled the merchant. A total of 131 merchants were disabled during this review.*
- *Treasury will review Marketplace store sales activity twice a year and disable stores that have not been used in the past 12 months. In addition, Treasury will work with the department representatives to ensure that they notify us when the store is no longer needed.*
- *Treasury is working with TouchNet to implement a process to automatically post Marketplace activity directly to the general ledger. In addition, Treasury has confirmed that there are no variances between the payment gateway and the bank account settlements. Treasury has now created a query that will allow reconciliation of the transactions in the payment gateway to the bank settlements on a monthly basis.*
- *Treasury will provide the Policy for Accepting Credit Card and Electronic Payments and other written procedures that describe the responsibilities and the process for setting up a merchant department and a Marketplace store. In addition, we will work with the Bursar to combine all procedures into one manual.*

Estimated Date of Implementation: *6/30/2017*

Person Responsible for Implementation: *Dr. Reda Bernoussi, Associate Controller; Karol Miller, Treasury Manager*

Conclusion

Based on the audit work performed, we conclude that controls within TouchNet application can be strengthened. Implementation of the recommendations outlined in this report will help enhance access controls and the efficiency of existing processes.

We appreciate the courtesy and cooperation received from the management and staff in the Offices of Budget and Finance, Web Services, and Information Technology as part of this audit.

Appendix: Priority Findings and Risk Matrix

Risk Level	Definition
Priority	High probability of occurrence that would significantly impact UT System and/or UT Dallas. Reported to UT System Audit, Compliance, and Management Review Committee (ACMRC). Priority findings reported to the ACMRC are defined as "*an issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.*"
High	Risks are considered to be substantially undesirable and pose a moderate to significant level of exposure to UT Dallas operations. Without appropriate controls, the risk will happen on a consistent basis.
Medium	The risks are considered to be undesirable and could moderately expose UT Dallas. Without appropriate controls, the risk will occur some of the time.
Low	Low probability of various risk factors occurring. Even with no controls, the exposure to UT Dallas will be minimal.