Office of Internal Audit

September 29, 2014

Dr. Kirk A. Calhoun, President
UT Health Northeast
11937 U. S. Hwy 271
Tyler, TX 75708

Dear Dr. Calhoun:

We have completed the Texas Administrative Code (TAC) §202 Online Banking Audit that was part of our fiscal year 2014 Audit Plan. The objective of the audit was to evaluate the adequacy of controls and separation of duties for tasks that are susceptible to fraudulent or other unauthorized activity within the institution’s online banking system. We found duties for online banking to be properly separated and overall internal controls were adequate to protect the institution’s information and assets. However, we identified several opportunities for strengthening controls within the system or related processes. Detailed results are included in the report.

This audit was conducted in accordance with guidelines set forth in The Institute of Internal Auditor's *International Standards for the Professional Practice of Internal Auditing*. We appreciate the assistance provided by management and other personnel and hope the information presented in our report is helpful.

Sincerely,

Kris I. Kavasch
Executive Director of Internal Audit

Enclosure

cc:
Mr. Joe Woelkers, Executive Vice President Institutional Operations and Chief of Staff joe.woelkers@uthct.edu
Mr. Vernon Moore, Senior Vice President, Chief Financial and Business Officer vernon.moores@uthct.edu
Ms. Annie Roten, Director of Accounting Services annie.roten@uthct.edu
Ms. Rose Mary Van Norman, Executive Director of Revenue Cycle Operations rosemary.vannorman@uthct.edu
Dr. Raymond S. Greenberg, UT System Executive Vice Chancellor for Health Affairs tmeloncon@utsystem.edu
Mr. J. Michael Peppers, UT System Chief Audit Executive systemauditoffice@utsystem.edu
Mr. Richard St. Onge, UT System Associate Vice Chancellor for Shared Services richardstonge@utsystem.edu
Ms. Dyan Hudson, UT System Assistant Director, Specialty Audit Services dhudson@utsystem.edu
Legislative Budget Board - ed.osner@lbb.state.tx.us
Governor - internalaudits@governor.state.tx.us
State Auditor’s Office - iaordinator@sao.state.tx.us
Sunset Advisory Commission - sunset@sunset.state.tx.us
TAC §202 Online Banking Audit

September 29, 2014

UT HEALTH NORTHEAST
OFFICE OF INTERNAL AUDIT
11937 US HIGHWAY 271
TYLER, TX 75708
TABLE OF CONTENTS

Executive Summary.................................................................................. 4

Background.................................................................................................. 4

Audit Objective.......................................................................................... 4

Audit Scope and Methodology................................................................. 5

Audit Results............................................................................................ 5

Conclusion............................................................................................... 13

Summary of Priority Findings................................................................. 14
Audit Report

Executive Summary
This audit focused on online banking security access processes and controls for UT Health Northeast’s primary accounts with JP Morgan Chase Bank. The objective of this audit was to evaluate the adequacy of controls and separation of duties for tasks that are susceptible to fraudulent or other unauthorized activity within the institution's online banking system, in accordance with TAC § 202.70. The scope of the audit was FY 2014.

We found that in combination the security features set up in the online banking system along with institutional controls promote protection of the institution’s assets and confidential information for online banking transactions considered to be susceptible to fraudulent or other unauthorized activity, in accordance with TAC §202.70 (8) requirements. Institutional processes and segregation of duties requirements and tightly controlled management of online banking system security administration are integral components of the internal control design that support this conclusion.

Several opportunities for improving processes and controls were identified for:
- Remote deposits
- Retiree insurance payments
- Compliance with UT System Policy #167 – Banking Services requirements

Detailed results are included within the report.

Background
This audit was completed as part of our FY 2014 Audit Plan. Texas Administrative Code (TAC) § 202.71(e) requires that each institution of higher education review, at least biennially, their information security program for compliance with TAC § 202 standards based on business risk management decisions, by individual(s) independent of the information security program and designated by the institution of higher education head or his or her designated representative(s). To comply with this biennial requirement and to focus our work on an area of higher risk for the institution this audit was focused on access security for the institution’s online banking system and related electronically processed transactions relative to the requirements of TAC §202.70 (8) which prescribes that institutions of higher education shall ensure adequate controls and separation of duties for tasks that are susceptible to fraudulent or other unauthorized activity.

Audit Objective
The objective was to evaluate the adequacy of controls and separation of duties for tasks that are susceptible to fraudulent or other unauthorized activity within the institution's online banking system, in accordance with TAC § 202.70.
Audit Scope and Methodology
The scope of the audit was FY 2014.

To achieve the audit objective, we performed the following procedures, among others:

- Reviewed the JP Morgan Chase Master and UT Health Northeast Agreements in effect along with pertinent documentation to gain an understanding of online banking services acquired.
- Reviewed the method and documentation in place for authorizing access to the online banking system and entitlements within the system.
- Identified the online banking system’s security features that contribute to the overall system of controls over the institution’s banking processes.
- Interviewed key individuals who administer institutional security features and process transactions within the online banking system.
- Tested a sample of users to determine the appropriateness of access granted relative to their job responsibilities.
- Tested a sample of users’ access log activity for a certain timeframe to identify any inappropriate access or activity.
- Reviewed manual and system controls and processes for a sample of transaction types we identified as higher risk for the institution to evaluate the design and implementation of controls over these electronic transactions. Electronic transactions and related process reviewed include lockbox deposits, remote deposits, ACH disbursements (including payroll and accounts payable transactions), and EFT/wire disbursements. We also reviewed processes in place for electronically processing retiree insurance payments.
- Reviewed UT Health Northeast processes and controls over banking activities to determine whether these were adequate to ensure compliance with UT System Policy #167 – Banking Services requirements that are specific to access and electronic transactions.

Our examination was conducted in accordance with guidelines set forth in The Institute of Internal Auditor’s International Standards for the Professional Practice of Internal Auditing.

Audit Results
In combination the security features set up in the online banking system along with institutional controls promote protection of the institution’s assets and confidential information for online banking transactions considered to be susceptible to fraudulent or other unauthorized activity, in accordance with TAC §202.70 (8) requirements. Detailed results are included below.

Online Banking Access
The only bank accounts for which UT Health Northeast fully utilizes online banking services are the JP Morgan Chase primary accounts so we focused our work on these services. Although we are not evaluating the adequacy of security for the Chase Online system that is controlled by the bank we determined that the Chase Online Banking system uses Secure Socket Layer (SSL)
technology to encrypt personal information such as user IDs, passwords and account information transmitted over the Internet. Some of the online banking system’s security features include password expiration, system time-outs, dual authorization and notifications. The bank sets up security administrator access for their customers based on authorization forms which must be signed by an authorized key official from the institution. Currently there are four UT Health Northeast security administrators who locally administer security for the institution. There are also two institutional Information Technology employees who have security access for managing the host-to-host activity. All users were properly authorized by the appropriate UT Health Northeast official for the access granted.

The bank delegates further security administration for the online banking system to UT Health Northeast and the employees who the institution authorized as security administrators for the system. We focused our review on security administration processes and controls for online banking activity which is managed by UT Health Northeast and their employees.

There are a total of 13 users, including the 4 security administrators, with active access to the UT Northeast accounts through the JP Morgan Chase Online Banking system. For users who have access which allows them to initiate or release transactions that disburse or transfer funds their system setup requires access via a unique username, password and token. The use of an assigned token provides an added measure of control in accessing the system since the number needed for entry changes every minute and the user must have the token in possession to be able to gain entry into the institution’s bank accounts. Users with view-only or reporting privileges access the system via a unique username and password only, which seems reasonable since these activities are considered lower risk.

One senior accountant has been assigned primary responsibility for security access requests and administration of access for users. The process deployed institutionally for granting access is somewhat informal with requests being made via e-mail correspondence initially; however, the granting of access and the dual controls required is well-documented within the online banking system. Controls have been set up in the system to require two security administrators to sign off to add or expand access for a user which provides an adequate level of oversight and segregation of duties to prevent one person from being able to add or expand access on their own. Access to the online banking system appears to have been properly controlled over time and granted only as required for an employee’s job responsibilities.

We tested security access and privileges in the system for a sample of six of the thirteen users who had various institutional responsibilities and levels of system access. Access for all six users tested appeared to be appropriate based upon their job responsibilities. Duties were adequately segregated and their setup in the system specifically disallows them from being able to release transactions they initiate. For four of the six users tested their access in the system appeared to be the most restrictive needed to perform their tasks. Two of the six users tested were granted some expanded access so they can serve as back-up personnel when others are absent which is reasonable to ensure transaction processing can remain uninterrupted to support operations. For users tested who were assigned RSA SecurID tokens, we found the tokens to be
physically secured and the token in use matched the token assigned. Documentation was available in the system to support that each user’s access was initiated and authorized by two separate security administrators. For new users who are given access to perform sensitive activities such as wire transfers, the system automatically generates an order for a token. The token is not functional until a security administrator in the system assigns the token to the user and a separate security administrator approves the token assignment in the system. There is also a feature in the system that allows a security administrator to initiate an order for a token but the order must be approved in the system by a separate security administrator for the order to be processed. Security administrators may also assign temporary token codes should a user’s token be damaged, stolen, lost or left at home. However, this process also requires two separate security administrators to initiate and approve the temporary token code assignment.

Access Logs
We reviewed all actions the six users in our sample performed in the online banking system for three separate dates (which occurred after the June 2014 upgrade of the system). We selected dates after the upgrade to ensure we were reviewing current system audit trail functionality and documentation. We found the audit trail documentation to be adequate and readily available to identify actions performed by users. For the six users tested no unusual or inappropriate activity was identified for the three dates reviewed.

Access via Non-Institutionally Owned Computers, Tablets and Mobile Phones
Users who have access to the JP Morgan Chase Online Banking System can access the institution’s bank accounts from institutionally owned and non-institutionally owned computers and mobile phones to process transactions as long as they have the proper credentials required by their security profile. UT Health Northeast has Information Technology security policies in place to protect the institution's assets and confidential or protected information. However, these policies and procedures do not address personally owned device security requirements and authorizations required for downloading and accessing applications that will be used for performing institutional business such as banking activities through a personally owned computer, tablet or mobile phone.

Recommendation #1: The Chief Information Officer should establish policies and procedures to address device security requirements when downloading and accessing applications which will be used for performing institutional business through non-institutionally owned computers and devices.

Management’s Response: The Chief Information Officer will research “Bring Your Own Device” (BYOD) policies and will develop a draft policy for the institution. Upon approval of the policy, the Information Technology Acceptable Use Policy will be updated to reference the institution’s “BYOD” policy.

Implementation Date: Draft Policy: November 30, 2014; Approved Policy: December 31, 2014
Design & Implementation (D&I) of Controls over Electronic Banking Transactions

**Lockbox Deposits**

UT Health Northeast acquires lockbox deposit services from JP Morgan Chase. Currently the institution has acquired services for four lockboxes for patient/customer payments including hospital, physician, patient and outpatient pharmacy payments. Insurance payers and patients send payments and supporting remittance data directly to the bank post office boxes where the bank processes the deposits to the institution’s bank account. The benefits of using this system is it provides for separation of duties over deposit transactions and deposits are made more expediently, improving cash flow. The bank scans the deposit documentation into the Receivables Edge system. Using the Receivables Edge module, UT Health Northeast staff access and download remittance and deposit information to record and reconcile these deposits in the institution’s patient, pharmacy, and financial information systems. Our work included review of users with access to lockbox data and institutional processes, controls and supporting documentation retained for these deposits. UT Health Northeast employees only handle the deposit information but not the actual payments which are received and processed by the bank. We determined the appropriate users have access to Receivables Edge and related lockbox deposit documentation and system controls are in place to protect this confidential information. It is important to note that we did not review lockbox deposit processes controlled and performed by the Chase Bank staff. We have no concerns about processes and controls deployed by UT Health Northeast staff for accessing and protecting lockbox deposit and patient related confidential information.

**D&I Testing:**

We tested the design and implementation of controls for a sample of two lockbox deposits made during the period under review. We found that duties were adequately segregated over these transactions. The bank received and processed the deposits to the bank account while UT Health Northeast employees processed the transactions to the financial and patient information systems. Documentation retained on file or available within the online banking system adequately supports these transactions and reflects they were valid business transactions.

**Remote Deposits**

UT Health Northeast utilizes the Chase Bank’s Image Deposit Direct services, which allows the institution to scan checks received directly by the institution and then transmit the data via the Internet for processing and then storage in the bank’s electronic image archives. The bank maintains 128-bit encryption and Secure Socket Layer (SSL) protocols with data encryption to keep these transactions secure. The system allows for scanning of deposits remotely to the bank and related reporting. A user does not need access to Chase Online Banking to be able to access the remote deposit system. Currently the Cashier’s Office is the only area that has the application software and scanner installed to be able to perform this function.

The bank delegates responsibility for administering security for the Image Deposit Direct system to UT Health Northeast and had granted security administrator access to a designated institutional employee; however, management did not reassign responsibility for administering
security for the JP Morgan Chase remote deposit scanning system after the resignation of the former Director of Business Operations which occurred in January 2014. When Audit requested security records for this system, we found there was no active security administrator for the system to provide security records, activate or deactivate access or expand privileges to the system as needed. In addition, we found that users of the system were sharing one generic username and password to gain access into the system which is contrary to the institution’s security policies that prohibits employees from sharing user identifications and passwords. During August 2014, the current Patient Financial Services Manager was successfully granted security administrator access to the remote scanning system and she set up security access for the users to require unique usernames and passwords.

There were no written policies and procedures for guiding the institution's remote deposit processes including but not limited to the method for gaining access to the Image Deposit Direct system, remote deposit daily procedures, documentation retention guidelines, security requirements for checks and reports that are retained on file for a period of time, method for responding to the bank's request for original items including the number of days allowed for the response, method for destroying remotely deposited checks and related reports, and system downtime procedures. However, prior to issuance of the audit report the Executive Director of Revenue Cycle Operations developed and implemented policies and procedures to resolve deficiencies. After management resolved the security and policy issues, we found that system and manual processes and controls over remote deposits are adequate, except as noted below:

- The UT Health Northeast Records Retention Schedule does not include the retention period record for remotely deposited original checks and related reports that must be retained on file for an acceptable period of time.
- Although original checks that have been deposited remotely are retained in a reasonably secure office location they are not kept locked in a cabinet or storage area to protect confidential information and reduce the risk for duplicate deposits.

Recommendation #2: The Patient Financial Services Manager should implement policies and procedures to improve security and controls over remote deposits by:

- Updating UT Health Northeast's official Records Retention Schedule to include records retention requirements for checks remotely deposited and related documents.
- Implementing processes to better secure the original checks that have been remotely deposited and are maintained on file for a period of time.

Management’s Response: The Patient Financial Services Manager immediately initiated requests for changes to improve physical security controls over remotely deposited checks. She has submitted a request to the institution’s Records Management Officer to update the Records Retention Schedule to include original check records maintained by the institution.

Implementation Date: November 30, 2014
D&I Testing
We tested the design and implementation of controls for two remotely scanned deposits and found that due to the use of a generic username and password we could not validate the user who performed the remote deposit activity within the Image Deposit Direct system reports reviewed. However, manual processes deployed assure a certain level of control by separating remote scanning, daily deposit reconciliation and monthly bank reconciliation duties among several employees. In addition, management has discontinued the process of sharing a username and password for the remote scanning system. We found that Chase Image Deposit Direct and Online Banking system documentation retained on file or available within the system was adequate to support that these were valid business transactions.

Electronic Funds Transfer Transactions
Automated Clearing House (ACH) Transfers
To process ACH accounts payable transactions, system access and duties are properly separated for the involvement of three employees in the transaction processing. One employee creates the wire transfer payments in the PeopleSoft system. A separate employee pulls the PeopleSoft reports and payment file for upload to the bank, accesses the online banking system and submits the payment file. Controls in the online banking system are set up to require a user other than the one who submitted the file to release the transaction before payment processing is complete. General ledger accountants, who are outside the Accounts Payable function, have access and primary responsibility for validating and releasing these transactions. Documentation is either maintained on file or available in the online banking system to validate duties are adequately segregated for these transactions and access for processing these transactions has been appropriately limited to employees who perform or release electronic payments and wires.

UT Health Northeast has ACH debit blocks in place for the JP Morgan Chase accounts. There is a very small list of vendors who have been pre-authorized to process ACH debits on the institution’s accounts. For these few, dollar limits are in place. Only those vendors who have been authorized to debit the institution’s accounts can do so. The bank denies transactions for all who attempt to debit the accounts but are not authorized.

For payroll transactions, one payroll employee has primary responsibility and access for processing payroll in the PeopleSoft system and uploading the payroll file to the Chase Online Banking system. System controls are in place to prohibit a user from initiating a transaction and also releasing it. In addition to the system controls, processes are in place for payroll management to release payroll transactions. For payroll transactions we found that the department does not print and maintain on file documentation from the Chase Online Banking system of who created, uploaded and released payroll transactions but this information is available within detailed user activity reports, except for dates prior to the Chase Online Banking System upgrade made in June 2014. Certain detail logs were not carried forward to the upgraded system but are available for transactions made after the upgrade.
D&I Testing:
We tested the design and implementation of controls for two accounts payable and two payroll ACH disbursements and found documentation was either retained on file or available within the online banking system to support that duties were adequately segregated when processing and releasing the transactions. Adequate source and system documentation was either retained on file or was accessible within the online banking system to support the transactions were authorized and were valid business transactions.

Credit Card payment processes and controls were excluded from the focus of this audit since we focused on transactions allowed via access to the JP Morgan Chase Online Banking System.

Wire Transfers
UT Health Northeast processes few wire transfers from the JP Morgan Chase accounts. The few wire transfers made from the primary accounts substantially are transfers to the UT System Board of Regents for UTIMCO investments or to UT System for amounts owed. Controls within the online banking system are set to require dual users to sign off before the wire transactions are released.

D&I Testing:
We tested the design and implementation of controls for one wire transfer made during the period and found documentation was either retained on file or available within the online banking system to support that duties were adequately segregated when processing and releasing the wire transaction. Documentation also supported that the transfer was properly authorized and was a valid business transaction.

We considered transfers of funds between the UT Health Northeast JP Morgan Chase deposit, demand, disbursement and payroll accounts less risky so those transfers of funds were not tested.

Retiree Insurance Payments
UT Health Northeast retirees provide personal debit and credit card information to the institution which is retained on file for paying the retiree’s personal portion of their monthly health insurance premiums. Although this confidential information is retained in secured office locations, controls need to be strengthened over this data.

Recommendation #3: The Patient Financial Services Manager and Director of Payroll Services need to implement controls for ensuring credit and debit card information that is kept on file within the institution is better secured within the offices where this data is maintained.

Management’s Response: The Patient Financial Services Manager and Director of Payroll Services immediately initiated requests for changes to improve physical security over credit and debit card information that is kept on file in their areas.

Implementation Date: November 30, 2014
Compliance with UT System Policy 167 – Banking Services

We compared UT Health Northeast policies and practices in place with certain sections of UT System Policy #167 – Banking Services which we believe to be applicable to security access and online banking transactions to determine whether requirements of this policy have been fully implemented by the institution. The table below displays the applicable policy sections reviewed along with the status of each.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Delegation of Authority</td>
<td>Compliant</td>
</tr>
<tr>
<td>7</td>
<td>Acquisition of Banking Services</td>
<td>Compliant</td>
</tr>
<tr>
<td>7.3</td>
<td>Primary Depository Services</td>
<td>Compliant</td>
</tr>
<tr>
<td>7.6</td>
<td>Standard Banking Depository Agreement</td>
<td>Compliant</td>
</tr>
<tr>
<td>7.9</td>
<td>Reconciliation of Accounts</td>
<td>Compliant</td>
</tr>
<tr>
<td>7.10</td>
<td>Identification of Unauthorized Accounts</td>
<td>Compliant</td>
</tr>
<tr>
<td>7.12</td>
<td>Acquisition of Banking Services:</td>
<td>Compliant</td>
</tr>
<tr>
<td>e.</td>
<td>ACH Transfer Dual Controls</td>
<td>Compliant</td>
</tr>
<tr>
<td>h.</td>
<td>Positive Pay</td>
<td>Compliant</td>
</tr>
<tr>
<td>m.</td>
<td>ACH Account Filters/Blocks</td>
<td>Compliant</td>
</tr>
<tr>
<td>9</td>
<td>Security Codes/PIN</td>
<td>Compliant</td>
</tr>
<tr>
<td>9.1</td>
<td>Securing Codes/PINS</td>
<td>Compliant</td>
</tr>
<tr>
<td>9.2</td>
<td>Changing Codes/PINS</td>
<td>Compliant</td>
</tr>
<tr>
<td>9.3</td>
<td>Relinquishing Codes/PINS</td>
<td>Compliant</td>
</tr>
<tr>
<td>9.4</td>
<td>Audit of Users</td>
<td>Not Compliant</td>
</tr>
<tr>
<td>10</td>
<td>Electronic Funds Transfers:</td>
<td>Compliant</td>
</tr>
<tr>
<td>10.1</td>
<td>Electronic Wires</td>
<td>Partially Compliant</td>
</tr>
<tr>
<td>10.7</td>
<td>Reporting Wires/Transfers to the Chief Business Officer</td>
<td>Compliant</td>
</tr>
<tr>
<td>10.8</td>
<td>Wire/Transfer Controls</td>
<td>Compliant</td>
</tr>
<tr>
<td>10.9</td>
<td>Standard Wire Transfer Requests</td>
<td>Compliant</td>
</tr>
<tr>
<td>10.13</td>
<td>Incoming Electronic Transactions</td>
<td>Compliant</td>
</tr>
</tbody>
</table>

Although UT Health Northeast has processes and controls in place to substantially comply with UTS Banking Services Policy #167 requirements for sections reviewed, the following deficiencies were identified:

- Section 9.4 requires for the CBO (Chief Business Officer) or controlling department heads to provide for an audit of authorized users and their assignments on no less than an annual basis. However, currently there is no process in place for an annual audit of authorized users and assignments.
- Section 10.1 requires for all money wires to be made electronically and preferably established on a repetitive basis if feasible. The policy requires electronic transactions for the withdrawal or transfer of funds from a banking institution to require action from a minimum of two authorized individuals. Hard controls are set up within the system to
require dual review and creation for repetitive transactions and for non-repetitive actions require dual initiation/release for wires or transfers as required by policy. However, a list of users authorized to initiate and release wires or transfers is not reported to or approved by the CBO or his designee at least annually as required by the policy.

To bring the institution into compliance, the Director of Accounting immediately developed a process for reviewing the online banking system authorized users and their entitlements and for providing the listing of users and their entitlements along with corresponding online banking system security access reports to the Senior Vice President, Chief Financial and Business Officer for his approval. To achieve compliance immediately, this process was performed in September 2014 prior to issuance of the audit report and reminders have been set up on the Director’s Outlook calendar for this process to be performed annually beginning in January 2015.

**Conclusion**

In combination the security features set up in the online banking system along with institutional controls promote protection of the institution’s assets and confidential information for online banking transactions considered to be susceptible to fraudulent or other unauthorized activity, in accordance with TAC §202.70 (8) requirements. Institutional processes and segregation of duties requirements and tightly controlled management of online banking system security administration are integral components of the internal control design that support this conclusion.

Kris I. Kavasch, Executive Director of Internal Audit
Summary of Priority Findings

According to The University of Texas System, a priority finding is 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. Standard factors for determining a priority finding have been established in three categories: namely, Organizational Controls, Quantitative Risks, and Qualitative Risks”.

In view of the above requirements, the TAC §202 Online Banking Audit had no priority findings.