Payment Acceptance Process

Audit Report No. R2511 | *January 24, 2025*

Audit and Advisory Services – *A Trusted Partner in Achieving University Excellence*
audit.utdallas.edu

Executive Summary

Audit Objective

To evaluate the effectiveness and adequacy of controls over the payment acceptance processes and compliance with the Payment Card Industry Data Security Standard (PCI DSS), including access controls, compliance with university policies and handling of credit cards, checks, and wire transfers.

Primary Risk Types

Finance
Information Technology

Controls and Strengths

- The University is primarily a cash-free environment which reduces the risk of cash fraud or theft.
- PCI DSS compliance is a shared responsibility of the Office of Budget & Finance (OBF), the Office of Information Technology (OIT), and the Information Security Office (ISO). This shared approach promotes compliance and includes information security professionals who stay up to date on security measures.
- The Treasury Department administers access to payment acceptance software which helps ensure centralized control and consistent application of financial policies, enhancing security and compliance.
- The workflow approval process in PeopleSoft for new stores or shops in the Marketplace system provides standardized tracking and compliance features, enhancing financial reliability and efficiency.

Overall Conclusion

The effectiveness and adequacy of controls over the payment acceptance processes and compliance with the Payment Card Industry Data Security Standard (PCI DSS), including access controls, compliance with university policies and handling of credit cards, checks, and wire transfers can be improved. Opportunities exist to improve controls related to monitoring, policies and procedures, and cost savings.

Observations by Risk Level

Management has reviewed the observations and has provided responses and expected implementation dates. Detailed information is included in the attached report.

Recommendation	Risk Level	Management's Implementation Date
1. Improve Credit Card and PCI Monitoring Procedures	**High**	November 30, 2025
2. Create Uniform Check Handling Procedures	**High**	August 31, 2025
3. Monitor Access to Payment Acceptance Applications	**Medium**	March 31, 2025
4. Improve Marketplace Process Controls	**Medium**	August 31, 2025
5. Create Bank Account Opening Procedures and Training for Employees that Oversee Student Organizations	**Low**	June 30, 2025
6. Consider Charging Credit Card Customers a Convenience Fee	**Low**	January 31, 2025

For details about the audit procedures, explanation of risk levels, and report distribution, please see Appendices A, B, and C, respectively, in the attached report.

Detailed Audit Results

The following are reportable observations and recommendations noting opportunities to enhance controls related to monitoring, policies and procedures, and cost savings. See Appendix B on page 13 for definitions of observation risk rankings.

1. ***Improve Credit Card and PCI Monitoring Processes***

High Risk: Without proper monitoring, communication, and training, there is an increased reputational risk and potential financial penalties and noncompliance with the PCI Data Security Standard in the event of a suspected or actual breach of cardholder data.

There are gaps in credit card and monitoring processes which could result in UTD not meeting contractual obligations with credit card payment processors that require PCI DSS compliance.

- Contracts and agreements are not reassessed each 12-month interval as required by PCI DSS 12.8.4 for changes in security, compliance, or operations, due to resource limitations in the Information Security Office (ISO).

- There is no formal communication process between the offices that are responsible for setting up vendors, monitoring merchant information, and ensuring compliance with PCI DSS. These offices are Purchasing, Treasury and Payment Services, and (ISO). Lack of communication between departments results in PCI DSS compliance requirements being overlooked. For example, an SAQ was found not completed when the Treasury Department had not yet loaded the vendor information into the PCI compliance portal, Aperia, and ISO was unaware. More frequent communication could reduce this timing discrepancy.

- Six out of 37 merchants were tested to determine if they had the appropriate PCI-required Self-Assessment Questionnaire (SAQ) completed.[1] One of the six SAQs was not fully completed due to human error.

- According to PCI DSS 12.6[2], organizations must have a formal security awareness training. The current Compliance Cybersecurity Awareness Training, which all UTD employees are required to take annually, has one slide with PCI

[1] https://docs-prv.pcisecuritystandards.org/SAQ%20(Assessment)/Instructions%20%26%20Guidance/SAQ-Instructions-Guidelines-PCI-DSS-v4-0-1.pdf
[2] PCI Standard 12.6 https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI_DSS-QRG-v4_0.pdf

information. While the overall training covers several cybersecurity components required by PCI, it is not sufficient to meet the training requirement for employees who handle credit cards.

Recommendation: To improve credit card and PCI monitoring processes, UTD should establish continuous monitoring of contracts, enhance communication between relevant offices, ensure accurate completion of PCI-required Self-Assessment Questionnaires (SAQ), and develop a formal PCI training program for those who handle credit card payments.

Management's Action Plan:

1. To ensure compliance with PCI DSS 12.8, ISO will maintain a current list of Third-Party Services Providers (TPSPs) and retain documentation confirming that the service provider is still meeting expectations for service delivery, each 12-month period.
2. ISO will host a quarterly PCI DSS coordination meeting among relevant units to promote open and productive communication.
3. SAQ questionnaires will be reviewed by two team members before submission to minimize the risk of human errors.
4. ISO will assign annual training specific to those who handle credit card payments.

Responsible Party Name and Title: Nate Howe, Chief Information Security Officer (CISO)

Estimated Date of Implementation: November 30, 2025

2. *Create Uniform Check Handling Procedures*

High Risk: Without uniform procedures in place, the risk of fraud, error, and theft is increased.

There is no uniform check handling process. Although the Treasury's website has limited guidelines on check handling[3], there is no monitoring performed by Treasury to ensure these guidelines are being followed.

Departments use the same process to deposit their checks, the Bank of America CashPro remote deposit system, but there are no formal standard operating procedures in place or training (aside from training on how to use the deposit system), which leads to departments following their inconsistent practices.

As CashPro only allows users to pull detailed information for the last three months, Audit & Advisory Services ran a report from May 31, 2024, through August 29, 2024. There were 2,016 deposits, totaling almost $10 million during this period. Of these deposits, there are 8 group types, each group type uses a different method to process their checks where the majority of processes don't require the cost center field to be inputted within CashPro.

Recommendation: The Treasury Department should create uniform check handling procedures and training, as well as perform monitoring processes to ensure check documentation is consistent throughout the University.

Management's Action Plan: Campus departments are required to follow the University's cash handling policies and procedures. In order to supplement our individual user training and the required CashPro training modules, Treasury will distribute a written training guide and a uniform check log template to all CashPro Remote Deposit users. In addition, Treasury will develop a monitoring process to verify that departments are following the appropriate deposit policies and procedures.

Responsible Party Name and Title: Karol Miller, Senior Director for Treasury & Payment Services

Estimated Date of Implementation: August 31, 2025

[3] https://finance.utdallas.edu/selling-goods-services/accepting-payments/

3. *Monitor Access to Payment Acceptance Applications*

Access to the different payment acceptance applications (Marketplace, TouchNet, and CashPro) should be monitored periodically. Based on access testing performed on 15 active user accounts from each application, we found instances where terminated employees still had access, a user who had more access than needed, and vendor administrator accounts that were no longer being used. The vendor administrator account was disabled after discovering the account was no longer in use.

Medium Risk: Unmonitored access could result in data breaches and operational disruptions.

Recommendation: Treasury should create a plan for periodically monitoring access to Marketplace, TouchNet, and CashPro.

Management's Action Plan: Treasury will enhance its user access monitoring process to prevent the events identified in this audit.

Responsible Party Name and Title: Karol Miller, Senior Director for Treasury & Payment Services

Estimated Date of Implementation: March 31, 2025

4. *Improve Marketplace Process Controls*

The Marketplace revenue reconciliation process is very manual, time-consuming, and thus subject to human error. Data is exported from Marketplace into a complicated spreadsheet where items are reconciled using formulas that span across multiple tabs; this is due to Marketplace currently lacking an effective report for exporting data.

Medium Risk: Having a manual and time-consuming reconciliation process can lead to increased errors and employee burnout.

Of 15 Marketplace revenue transactions tested, two departments could not provide supporting documentation. Also, one transaction was coded to the wrong cost center, due to the complication of the reconciliation spreadsheet, and there was no corrective journal entry to move the revenue to the correct cost center. Note: Internal Audit confirmed that a corrective journal entry was made after it was noted during our procedures.

Recommendation: To improve Marketplace process controls, UTD should automate the revenue reconciliation process to reduce manual effort and human error, and ensure all transactions are properly documented and coded to the correct cost centers with appropriate corrective actions taken when necessary.

Management's Action Plan: The Treasury team is currently evaluating several options for streamlining the process for reconciling and posting Marketplace transactions. Although full automation may not be possible, these improvements are intended to reduce the manual effort required by the Treasury team.

While Treasury reconciles the cash received, departments are responsible for reconciling and maintaining documentation for their Marketplace revenue. If they determine that there are any discrepancies in Marketplace journals, they are expected to contact Treasury for assistance with initiating a correction. Treasury will update the Marketplace reference material that is provided to store owners to ensure that these requirements are clearly documented.

Responsible Party Name and Title: Karol Miller, Senior Director for Treasury & Payment Services

Estimated Date of Implementation: August 31, 2025

5. *Create Bank Account Opening Procedures and Training for Employees that Oversee Student Organizations*

Low Risk: Individuals or organizations could open unauthorized bank accounts in UTD's name**.**

UTD is not notified when individuals or organizations create a bank account at Bank of America that uses the UTD name; this has happened with student organizations. Often, the Treasury Department notices this when student organizations use UTD's mailing address or employer identification number (tax ID), and they receive related bank statements. Currently, there is no guidance available to discourage the opening of bank accounts using UTD's name.

Recommendation: UTD should create procedures and training for employees who oversee student organizations to ensure student organizations are not opening bank accounts using UTD's name or tax ID.

Management's Action Plan: The Student Organization Center provides training for Student Orgs and maintains a Student Organization Manual that provides information regarding the use of UTD's name. Treasury will work with the Director of Student Development to ensure that the manual also includes guidance for opening bank accounts and a notification that they should not use the University's tax ID.

Since banking privacy laws prevent us from obtaining information about bank accounts that do not belong to the University, Treasury will continue to monitor notifications provided by UTD's banks for any accounts that are opened using our tax ID.

Responsible Party Name and Title: Karol Miller, Senior Director for Treasury & Payment Services

Estimated Date of Implementation: June 30, 2025

6. ***Consider Charging Credit Card Customers a Convenience Fee***

UTD had over $10 million in credit card revenues in FY24. UTD departments paid over $271K in credit card fees, because these fees were not charged to the customers. In an environment with limited budgets, this could be a potential cost savings.

Low Risk: Not charging the credit card customers for bank processing fees can result in increased expenses to the university as well as increased costs results from the time spent distributing the fees across the campus.

The current process to allocate credit card fees amongst the various departments is very manual and time-consuming. Due to limitations, it is not possible to charge each department actual credit card fees. Instead, they are charged a percentage of the total credit card fee based on their total departmental monthly revenue, not just credit card revenue.

Recommendation: The Treasury Department should work with Executive Leadership to consider creating and implementing a plan to begin charging UTD customers a credit card convenience fee.

Management's Action Plan: Treasury will forward the recommendation to the University's Senior Management for their consideration.

Responsible Party Name and Title: Karol Miller, Senior Director for Treasury & Payment Services

Estimated Date of Implementation: January 31, 2025

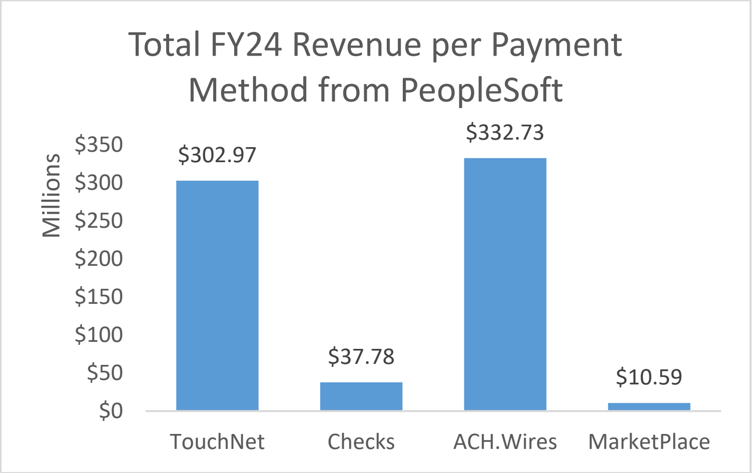
Overall Conclusion

The effectiveness and adequacy of controls over the payment acceptance processes and compliance with the Payment Card Industry Data Security Standards (PCI DSS), including access controls, compliance with university policies and handling of credit cards, checks, and wire transfers can be improved. Opportunities exist to improve controls related to monitoring, policies and procedures, and cost savings.

Appendix A: Information Related to the Audit

Background

UTDBP3040 – Payment Acceptance Policy provides guidance regarding the requirements for departments who accept payments. UTD strives to be a cash-free environment and receives payments primarily through checks, credit card merchants, Automated Clearing House (ACH)/electronic funds transfers (EFT), and wire transfers. The audit only reviewed these areas, which total $684.07 million. The Treasury and Payment Services Department, reporting to the Vice President for Budget and Finance, manages the operational tasks of payment acceptance. The Information Security Office (ISO), reporting to the Vice President and Chief of Staff, monitors for compliance with Payment Card Industry Data Security Standard (PCI DSS) for credit card merchants at UTD.



Checks are deposited through a remote deposit scanner via the Bank of America system CashPro. Various departments on campus have these scanners and can scan in any checks they may receive.

Based on information provided by Treasury, a total of 37 unique merchant IDs are associated with the acceptance of credit cards across UTD, supported by merchants such as TouchNet, CBORD, and Authorize.net. From this information, it was determined that TouchNet was the main vendor used at UTD for online credit card sales and because of this IA focused the audit procedures on TouchNet revenues. The primary merchant used is TouchNet, which also manages Marketplace. TouchNet collects student tuition payments, and Marketplace collects payments for goods or services offered by various UTD departments.

ACH and wire transfers are used for student loan repayments, gifts, sponsored projects, goods and services payments, and various revenues.

Objective

To evaluate the effectiveness and adequacy of controls over the payment acceptance processes and compliance with the Payment Card Industry Data Security Standards (PCI DSS), including access controls, compliance with university policies and handling of credit cards, checks, and wire transfers.

Scope

The scope of the audit was fiscal year 2024. Fieldwork was conducted from August 15, 2024, and the audit concluded on November 18, 2024.

Methodology

The audit was conducted in conformance with the 2017 Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*. Additionally, we conducted the audit in conformance with generally accepted government auditing standards (GAGAS). Both standards are required by the Texas Internal Auditing Act, and they require that we plan and perform the audit to obtain sufficient, proper 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 Office of Audit and Consulting Services is independent in based on both standards for internal auditors.

GAGAS also requires that auditors assess internal control when it is significant to the audit objectives. We used the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework in assessing internal controls[4].

Our audit procedures included interviews, observations of processes, reviews of documentation, and testing. The following table outlines our audit procedures and overall controls assessment for each of the audit area objectives performed.

Audit Area	Procedures	Observation Related to the Audit Area
Gaining an Understanding	• Gained an understanding of processes related to payment acceptance and Payment Card Industry Data Security Standards (PCI DSS), by	Observation 6

[4] http://www.coso.org

Audit Area	Procedures	Observation Related to the Audit Area
	conducting interviews with personnel. • Performed a risk assessment to identify areas of high risk within operations, and focused audit procedures on those risks.	
PCI Compliance/Credit Card Handling	Tested Self-Assessment Questionnaires (SAQs), access, and transactions to ensure credit card processes are in compliance with the following policies: UTDBP3040 Payment Acceptance Policy and UTDBP3035 Credit Card Acceptance Policy.	Observations 1, 2, 4, & 5
Check Handling	Tested transactions to ensure check revenue is in compliance with UTD3040 Payment Acceptance Policy and CashPro access is granted based on the principle of least privilege.	Observations 3 & 4
Wire Transfers/ACH	Tested transactions to ensure compliance with UTD3040 Payment Acceptance Policy.	N/A

Follow-up Procedures

Though management is responsible for implementing the course of action outlined in the response, we will follow up on the status of implementation after the expected implementation dates. Requests for extension to the implementation dates may require approval from the UT Dallas Audit Committee. This process will help enhance accountability and ensure that prompt action is taken to address the observations.

Appendix B: Observation Risk Rankings

Audit observations are ranked according to the following definitions, consistent with UT System Audit Office guidance.

Risk Level	Definition
Priority	If not addressed immediately, a priority observation has a significant probability to directly affect the achievement of a strategic or important operational objective of UT Dallas or the UT System as a whole. These observations are reported to and tracked by the UT System Audit, Compliance, and Risk Management Committee (ACRMC).
High	High-risk observations are substantially undesirable and pose a high probability of adverse effects to UT Dallas either as a whole or to a division/school/department level.
Medium	Medium-risk observations are considered to have a moderate probability of adverse effects to UT Dallas either as a whole or to a division/school/department level.
Low	Low-risk observations are considered to have a low probability of adverse effects to UT Dallas either as a whole or to a division/school/department level.
Minimal	Some recommendations made during an audit are considered of minimal risk, and the observations are verbally shared with management during the audit or at the concluding meeting.

Appendix C: Report Submission and Distribution

We thank the Treasury and Payment Services as well as the Information Security Office management and staff for their support, courtesy, and cooperation provided throughout this audit.

Respectfully Submitted,

DocuSigned by:
Toni Stephens
26B49AE7B918458...

Toni Stephens, CPA, CIA, CRMA, Chief Audit Executive

Distribution List

Members and ex-officio members of the UT Dallas Institutional Audit Committee

Responsible Vice President
Dr. Rafael Martin (Observation 1)
Mr. Terry Pankratz, Vice President for Budget and Finance (Observations 2-6)

Persons Responsible for Implementing Recommendations:
Mr. Nate Howe, Chief Information Security Officer (Observation 1)
Ms. Karol Miller, Senior Director for Treasury & Payment Services (Observations 2-6)

Other Interested Parties
Mr. Orkun Torus, Associate Vice President of Budget and Finance, Budget
Dr. Brian Bernoussi, Associate Vice President of Budget and Finance, Financial Management Services
Ms. Jennifer Mayes, Financial Compliance Manager

External Parties

- The University of Texas System Audit Office
- Legislative Budget Board
- Governor’s Office
- State Auditor’s Office

Engagement Team
Project Manager: Luis Carrera, CPA, CIA, CISA, IT Audit Manager
Project Leader: Caitlin Cummins, Internal Auditor III