

# OFFICE OF THE STATE AUDITOR

---

# DIANA DIZOGLIO

Official Audit Report – Issued April 19, 2024

---

## University of Massachusetts Lowell

For the period July 1, 2020 through December 31, 2021



# OFFICE OF THE STATE AUDITOR

---

# DIANA DIZOGLIO

April 19, 2024

Dr. Julie Chen, Chancellor  
University of Massachusetts Lowell  
220 Pawtucket Street, Suite 400  
Lowell, MA 01854

Dear Dr. Chen:

I am pleased to provide to you the results of the enclosed performance audit of the University of Massachusetts Lowell. As is typically the case, this report details the audit objectives, scope, methodology, findings, and recommendations for the audit period, July 1, 2020 through December 31, 2021. As you know, my audit team discussed the contents of this report with university management. This report reflects those comments.

I appreciate you and all your efforts at the University of Massachusetts Lowell. The cooperation and assistance provided to my staff during the audit went a long way toward a smooth process. Thank you for encouraging and making available your team. I am available to discuss this audit if you or your team have any questions.

Best regards,



Diana DiZoglio  
Auditor of the Commonwealth

cc: Martin T. Meehan, President of the University of Massachusetts  
Stephen R. Karam, Chair of the Board of Trustees of the University of Massachusetts  
Dr. Noe Ortega, Commissioner of the Massachusetts Department of Higher Education

---

## TABLE OF CONTENTS

<b>EXECUTIVE SUMMARY .....</b>	<b>1</b>
<b>OVERVIEW OF AUDITED ENTITY .....</b>	<b>2</b>
<b>AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY .....</b>	<b>5</b>
<b>DETAILED AUDIT FINDINGS WITH AUDITEE’S RESPONSE.....</b>	<b>13</b>
1. The University of Massachusetts Lowell’s bank card transactions did not always comply with University of Massachusetts system policies and standards. ....	13
2. The University of Massachusetts Lowell’s cybersecurity awareness training documentation was missing crucial information, and the university did not ensure that all nonfaculty employees completed cybersecurity awareness training. ....	19

## EXECUTIVE SUMMARY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor has conducted a performance audit of the University of Massachusetts (UMass) Lowell for the period July 1, 2020 through December 31, 2021.

In this performance audit, we determined whether UMass Lowell executed all bank card purchases in accordance with Sections II(A), II(D), III(A), and III(B) of the “Administrative Standards for the Business Expense Policy” within Appendix C of the “University of Massachusetts Business and Travel Expense Policy” (document T92-031) and Sections 2, 4–8, 11, 12, 15, and 21 of the UMass Bank Card Use Standard. We also determined whether UMass Lowell adhered to its “Security Awareness Policy IT-5-112” regarding cybersecurity awareness training for nonfaculty employees.

Below is a summary of our findings and recommendations, with links to each page listed.

<b>Finding 1</b> <b>Page <a href="#">13</a></b>	UMass Lowell’s bank card transactions did not always comply with UMass system policies and standards.
<b>Recommendations</b> <b>Page <a href="#">16</a></b>	<ol style="list-style-type: none"><li>1. UMass Lowell should ensure that cardholders reconcile and upload all bank statements and supporting documents into the UMass system’s online bank card transaction repository within 30 days of the bank statement date.</li><li>2. UMass Lowell should ensure that each bank card transaction receipt captures the full business purpose and that all required information is on the receipt. If this is not feasible within the requirements of the current standard, then the UMass system should update the UMass Bank Card Use Standard to reflect appropriate and feasible requirements.</li><li>3. UMass Lowell should ensure that state sales tax is not charged when bank card purchases are made by cardholders. If this is not feasible within the requirements of the current standard, then the UMass system should update the UMass Bank Card Use Standard to reflect appropriate and feasible requirements.</li><li>4. UMass Lowell should ensure that travel authorization numbers are referenced on the bank statement and receipt(s). If this is not feasible within the requirements of the current standard, then the UMass system should update the UMass Bank Card Use Standard to reflect appropriate and feasible requirements.</li></ol>
<b>Finding 2</b> <b>Page <a href="#">19</a></b>	UMass Lowell’s cybersecurity awareness training documentation was missing crucial information, and the university did not ensure that all nonfaculty employees completed cybersecurity awareness training.
<b>Recommendations</b> <b>Page <a href="#">20</a></b>	<ol style="list-style-type: none"><li>1. UMass Lowell should configure its cybersecurity awareness training platform so that it has the ability to monitor the assignment and completion of the trainings.</li><li>2. UMass Lowell should ensure that its nonfaculty employees complete cybersecurity awareness training when they are hired and annually thereafter.</li><li>3. UMass Lowell should retain sufficient cybersecurity awareness training documentation.</li></ol>

---

## OVERVIEW OF AUDITED ENTITY

The University of Massachusetts (UMass) Lowell is one of five campuses (Amherst, Boston, Dartmouth, Lowell, and the Chan Medical School in Worcester) in the UMass system. The UMass system was established under Section 1 of Chapter 75 of the Massachusetts General Laws and is overseen by a president. Each campus is overseen by a chancellor. The president and a 22-member board of trustees provide governance to the UMass system. UMass Lowell is a member of the Massachusetts public higher education system, which consists of 15 community colleges, nine state universities, and the five UMass campuses. It is located at 1 University Avenue in Lowell, with a satellite campus in Haverhill.

According to UMass Lowell's website,

*The chancellor works in close collaboration with the University of Massachusetts Trustees, the University of Massachusetts President's Office, the UMASS Lowell faculty, staff and students as well as community leaders in government, business, education, and the nonprofit sector to ensure that the campus is a vital and engaged partner, an effective leader and a responsible steward of the state's mission for public higher education.*

During fiscal year 2021, UMass Lowell had a student population of approximately 14,855, a faculty employee population of 783, and a nonfaculty employee population of 999. During fiscal year 2021, UMass Lowell had \$474,927,000 in revenue, which included \$133,768,000 in state appropriations, and \$463,883,000 in expenses.

According to UMass Lowell's website,

*The University of Massachusetts Lowell is a nationally ranked public research university committed to excellence in teaching, research and community engagement. We strive to prepare students to succeed in college and to become lifelong learners and informed citizens in a global environment. UMass Lowell offers affordable, experience-based undergraduate and graduate academic programs taught by internationally recognized faculty who conduct research to expand the horizons of knowledge and sustainable practices. The programs span and interconnect the disciplines of business, education, engineering, fine arts, health, humanities, sciences and social sciences. The university continues to build on its founding tradition of innovation, entrepreneurship and partnerships with industry and the community to address challenges facing the region and the world.*

---

## Unified Procurement Services Team

In January 2020, the UMass system established the Unified Procurement Services Team (UPST). According to the website for the Office of the President of the UMass system,

*The Unified Procurement Services Team ("UPST") is established and under the direction of the Chief Procurement Officer and is responsible for the implementation of the Standards applicable to the University's campuses and the President's Office. . . .*

*The Unified Procurement Services Team (UPST) was created to provide purchasing, accounts payable, bid execution (sourcing), contracts, and supplier management services to the University of Massachusetts and our partner/ supplier community. We are professionals gathered from all the various UMass campuses to provide high-quality service while driving transaction efficiency.*

*We manage an average of \$1 billion in third-party spend annually, and 17,000+ suppliers/partners.*

The UPST also administers the UMass Bank Card Program, which is described below, for the UMass system.

## UMass Bank Card Program

The rollout of the UMass Bank Card Program started in October 2020 and finished in January 2021. This UMass Bank Card Program transitioned the UMass system away from using a procurement card administered through Citibank to using a bank card administered through U.S. Bank.

According to the UMass Bank Card Use Standard,

*The purpose of the University of Massachusetts Bank Card program . . . is to offer a payment method for those vendors that do not accept a Purchase Order, a mechanism for emergency purchases, and a payment method in lieu of employee Travel reimbursement. . . . The UMass Bank Card is a commercial credit card. The card works in much the same way as your personal credit card except the monthly statement amount is paid for by the University. Each card has specific spending limits and card controls.*

The UPST issues these bank cards to employees who are first approved by their UMass Lowell department supervisor or manager and have, according to the UMass Bank Card Use Standard, "a frequent need to make purchases on behalf of their department."

After the transition from the procurement card to the bank card, the UMass Bank Card Program created a new process for reviewing cardholders' bank statement reconciliations. Previously, for Citibank cardholders, the process consisted of submitting all reconciled bank statements and supporting

documents<sup>1</sup> to UMass Lowell management, who then kept these documents on file. The new process for U.S. Bank cardholders is to upload all reconciled bank statements and supporting documents into the UMass system's online bank card transaction repository.<sup>2</sup> According to the UMass Bank Card Use Standard, the steps the cardholder must take include the following.

1. After the cardholder reconciles their monthly bank statement, they fill out the bank card form in the UMass system's online bank card transaction repository. This opens a requisition, which is a folder that contains any supporting documents, within the bank card transaction repository.
2. The cardholder then uploads the bank statement and any supporting documents to the requisition.
3. The cardholder submits their requisition to their UMass Lowell supervisor for approval. (Both of these actions occur in the bank card transaction repository.) The bank card transaction repository timestamps the requisition upon its submission. The requisition, which should be submitted within 30 days of the bank statement date, is considered complete after management approves it, at which time the bank card transaction repository timestamps the requisition again.

During the audit period, there were 511 UMass Lowell cardholders, whose spending on items and services totaled approximately \$4.1 million.

## Cybersecurity Awareness Training

UMass Lowell has a formal cybersecurity awareness training policy in place that requires all staff members to complete an initial cybersecurity awareness training upon hire and an annual refresher training thereafter. UMass Lowell provides cybersecurity awareness training through a web-based, third-party platform. UMass Lowell's chief information security officer customizes the training to staff members based on their department and job responsibilities. The cybersecurity awareness training platform records and tracks the assignment and completion status of each staff member's initial and annual cybersecurity awareness trainings.

---

1. Supporting documents consist of various documents relevant to a particular reconciliation or transaction, such as invoices, receipts, purchase logs, travel authorizations, general ledger screenshots, etc.

2. According to the UPST's "Upload Bank Card Statement and Receipts in [the UMass system's Online Bank Card Transaction Repository]" document, the bank card transaction repository is "for Bank Card transactions, statements, and receipts. Statements and supporting documents are archived within [the bank card transaction repository], where they are available as needed by the Department, Financial Services or Grants, and Auditors."

## AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor has conducted a performance audit of certain activities of the University of Massachusetts (UMass) Lowell for the period July 1, 2020 through December 31, 2021.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Below is a list of our audit objectives, indicating each question we intended our audit to answer; the conclusion we reached regarding each objective; and, if applicable, where each objective is discussed in the audit findings.

Objective	Conclusion
1. Did UMass Lowell execute all bank card purchases in accordance with Sections II(A), II(D), III(A), and III(B) of the “Administrative Standards for the Business Expense Policy” within Appendix C of the “University of Massachusetts Business and Travel Expense Policy” (document T92-031) and Sections 2, 4–8, 11, 12, 15, and 21 of the UMass Bank Card Use Standard?	<b>No; see Finding <u>1</u></b>
2. Did UMass Lowell adhere to its “Security Awareness Policy IT-5-112” regarding cybersecurity awareness training for nonfaculty employees?	<b>No; see Finding <u>2</u></b>

To accomplish our audit objectives, we gained an understanding of the aspects of UMass Lowell’s internal control environment that we determined to be relevant to our objectives by reviewing applicable UMass system policies and procedures and by interviewing UMass Lowell and UMass system management.

To obtain sufficient, appropriate evidence to address our audit objectives, we performed the following procedures.

### Bank Card Purchases

To determine whether UMass Lowell executed bank card purchases in accordance with Sections II(A), II(D), III(A), and III(B) of the “Administrative Standards for the Business Expense Policy” within Appendix C of the “University of Massachusetts Business and Travel Expense Policy” and Sections 2, 4–8, 11, 12, 15,



and 21 of the UMass Bank Card Use Standard, we distributed the total population of 19,556 bank card transactions made during the audit period, totaling \$4,137,309, into the following five categories.

Category Number	Category Description	Number of Transactions	Total Dollar Value of Transactions
1	\$7,500 or Higher	9	\$ 146,432
2	Transactions with Shared Transaction Numbers*	140	29,961
3	Amazon, eBay, and PayPal	5,106	575,330
4	Food and Groceries	678	72,494
5	All Remaining Transactions**	13,623	3,313,091
	Total†	<u>19,556</u>	<u>\$ 4,137,309</u>

\* Each UMass Lowell bank card transaction has a unique transaction number assigned to it by the bank during the transaction process. The transactions in this category are ones that we found that shared the same transaction number with one or more other transactions. Transactions with shared transaction numbers can be attributed to various situations, such as splitting the cost of purchased items with multiple departments. For these transactions, our testing found that only one transaction amount was charged to UMass Lowell's General Ledger.

\*\* This includes transactions that did not fit into the four previous categories. Examples include laboratory materials, books, subscriptions, hardware, and marketing items.

† Discrepancy in total is due to rounding.

The method we used to select our sample, which consisted of 110 transactions and totaled \$167,312, is as follows:

- From category one, we selected all 9 transactions, which totaled \$146,432.
- From category two, we judgmentally selected 10 transactions (out of 140 transactions), which totaled \$8,516.
- From categories three through five, we used a 95% confidence level,<sup>3</sup> a 50% expected error rate,<sup>4</sup> and a 22% desired precision range<sup>5</sup> to determine that our sample should consist of, at a minimum, 85 transactions. We then increased the sample size to 91 transactions and used Audit Command Language software<sup>6</sup> to randomly select the following:

3. Confidence level is a mathematically based measure of the auditor's assurance that the sample results (statistic) are representative of the population (parameter), expressed as a percentage. A 95% confidence level means that 95 out of 100 times, the statistics accurately represent the larger population.
4. Expected error rate is the number of errors that are expected in the population, expressed as a percentage. It is based on the auditor's knowledge of factors such as prior audit results, the understanding of controls gained in planning, or a probe sample. In this case, we are assuming there are relatively frequent errors in the data provided to us by the auditee.
5. The desired precision range defines the area of likely values within which the true population value should lie. The lower or higher the precision range, the larger or smaller, respectively, the sample size would be. Based on our understanding of the population of bank card transactions and the expected error rate of 50%, we chose a 22% desired precision range.
6. Audit Command Language software is a data extraction and analysis software used by auditors to analyze data populations, select sample sizes, identify trends, and highlight potential areas of concern.

- From category three, we selected 45 transactions (out of 5,106 transactions), which totaled \$5,253.
- From category four, we selected 6 transactions (out of 678 transactions), which totaled \$339.
- From category five, we selected 40 transactions (out of 13,623 transactions), which totaled \$6,772.

Our sample of 110 transactions included 21 transactions that were made using Citibank procurement cards and 89 transactions that were made using U.S. Bank cards. For these transactions, we performed the following procedures.

### **Submission of Bank Card Transaction Documents**

To determine whether cardholders completed Citibank statement reconciliations and submitted relevant receipts and other supporting documents to UMass Lowell management, we requested that UMass Lowell management provide us with hard copies of these documents. Once we received these documents, we recorded which documents were submitted to UMass Lowell management and which were missing.

To determine whether UMass Lowell cardholders completed timely U.S. Bank statement reconciliations and uploaded the corresponding bank statements and any supporting documents into the UMass system's online bank card transaction repository, we met with a UPST bank card manager and observed them locating all of the requisitions for the transactions in our sample in the bank card transaction repository. We recorded the creation dates of the relevant requisitions. Then we took screenshots of each bank statement and any supporting documents within the bank card transaction repository. If any transactions in our sample were missing bank statements or receipts, because those were required to be submitted, the UPST member obtained those from the cardholders. Once all documents related to our sample were provided to us, we recorded which documents were uploaded and, for those not uploaded, which documents were retrieved from the cardholder or were attempted to be retrieved but were still missing. By comparing each requisition's creation date and the bank statement date, we determined whether the requisition was created within 30 days after the bank statement date.

## **Information on Receipts and Bank Statements**

To determine whether each receipt in our sample of 110 transactions contained the vendor name, the description of the item or service purchased, the transaction date, the transaction total, and the last four digits of the bank card used to make the purchase, we inspected each receipt and noted any missing information.

To determine whether each receipt related to our sample of 110 transactions contained the start and expiration dates for purchased subscriptions (e.g., online data storage and marketing software), we first determined whether the transactions were for subscriptions by inspecting the receipts for descriptions of what was purchased. We then inspected each receipt for subscription start and end dates, if applicable.

To determine whether each receipt related to our sample of 110 transactions contained a documented business purpose, if not self-evident, we inspected each receipt and/or purchase log for a documented business purpose. When a transaction's documented business purpose was not indicated on either its corresponding receipt or purchase log, we used the Human Resources Compensation Management System (HR/CMS), which is the Commonwealth's official payroll system, to identify the cardholder's title. We inspected the relevant receipts and purchase logs for the type of item or service purchased. We then determined whether the description of the items or services purchased were typical purchases for that cardholder's title and department. We also met with UMass system and UMass Lowell management to ask about the business purposes for transactions that did not have documented business purposes on their corresponding receipts and/or purchase logs.

To determine whether each of the 110 transactions in our sample was related to the goals and mission of UMass Lowell, we inspected the bank statement and supporting documents to identify the type of purchase. We considered whether the purchase had a documented business purpose and was approved by the cardholder's supervisor. We also met with UMass system and UMass Lowell management to inquire about how the purchases related to the goals and mission the UMass Lowell.

To determine whether each of the 110 transactions in our sample required a travel authorization number—a reference number indicating that the travel was preapproved—to be documented on the related receipt(s) and bank statement, we identified which transactions were travel-related by inspecting the supporting documents for vendor names and transaction descriptions related to travel

(i.e., airlines, lodging, car rentals, and gasoline). In addition, we inspected the supporting documents for a notation made by a UMass Lowell employee that would confirm that the transaction was for travel-related business purposes. We then inspected each receipt and bank statement for a travel authorization number, if applicable.

To determine whether cardholders and supervisors signed the bank statements related to the 110 transactions in our sample, we inspected the bank statements for these signatures.

### **Allowable Purchases**

To determine whether each of the 110 transactions in our sample was for an allowable purchase, we inspected the supporting documents for the type of item(s) or service(s) purchased. To determine whether a transaction was a foreign expense,<sup>7</sup> we inspected each receipt for a vendor address outside of the United States and for any foreign expense fees. To determine whether each transaction was for out-of-state travel, we inspected the relevant supporting documents for vendor addresses that were out of state and for any notations that the transaction was for travel or travel-related meals.

To determine whether each transaction was related to a business function, we inspected the relevant receipts and purchase logs for purchases such as conference registration fees, conference supplies (e.g., table settings, flowers, and snacks), and for any notation that these purchases were for a business function. We also inspected each receipt to determine whether sales tax was charged. If sales tax was charged, we inspected the related bank statement and general ledger to determine whether sales tax was refunded by the vendor to UMass Lowell. For each transaction that was made during the audit period by a cardholder whose employment was terminated during the audit period, we inspected the related bank statement for purchase dates and compared these dates to the cardholder's termination date, which we obtained from HR/CMS.

Please see Finding 1 for information about the results of this testing.

---

7. A foreign expense is a transaction made with a vendor or business that is outside of the United States.

## Cybersecurity Awareness Training

To determine whether UMass Lowell adhered to its “Security Awareness Policy IT-5-112” and provided cybersecurity awareness training to nonfaculty employees, using the population of 1,137 nonfaculty employees who had computer network access during the audit period, we took the following actions.

We distributed the 1,137 nonfaculty employees into the following two categories: 121 nonfaculty employees who were hired during the audit period (i.e., newly hired employees) and were required to complete initial cybersecurity awareness training, and 1,016 nonfaculty employees who were hired before the audit period (i.e., existing nonfaculty employees) and were required to complete annual cybersecurity awareness training during the audit period. We selected a random, statistical sample of 80 nonfaculty employees from our population of 1,137, using a 95% confidence level, 0% expected error rate, and a 5% tolerable error rate.<sup>8</sup> The sample of 80 consisted of 20 newly hired employees and 60 existing nonfaculty employees. We obtained evidence (i.e., screenshots of employee cybersecurity awareness training activity) from UMass Lowell’s cybersecurity awareness training platform, which assigns and tracks the completion of cybersecurity awareness training, and we determined whether our sampled nonfaculty employees completed the required initial or annual cybersecurity awareness training by inspecting each assignment date and completion date recorded in UMass Lowell’s cybersecurity awareness training platform.

Please see Finding 2 for information about the results of this testing.

## Data Reliability Assessment

To determine the reliability of the bank card transaction data, we interviewed UMass system management who were knowledgeable about the data. We also reviewed the access controls for UMass Lowell’s computer network. To determine the completeness of the bank card transaction data, we observed the UPST bank card manager query the UMass system’s finance system and extract 28,152 bank card transactions that were made during the audit period. The UPST bank card manager then provided these 28,152 bank card transactions to us in a Microsoft Excel spreadsheet. We ensured that the total number of bank card transactions we observed within the finance system matched the total number of bank card transactions from the Excel spreadsheet. We inspected the bank card transaction data for hidden rows

---

8. The tolerable error rate (which is expressed as a percentage) is the maximum error in the population that is acceptable while still using the sample to conclude that the results from the sample have achieved the objective.

and columns, embedded data,<sup>9</sup> and invisible content. We also inspected the bank card transaction data for duplicates, identifying whether a transaction number appeared more than once within the data. We also met with UMass system management to understand any inconsistencies we found while analyzing the bank card transaction data.

To determine the completeness of the population of 28,152 transactions, we judgmentally selected a sample of 20 transactions listed on bank statements and compared them to the 28,152 bank card transactions that were made during the audit period, which were listed in the UMass system's finance system data. To determine the accuracy of this population, we judgmentally selected a sample of 20 bank card transactions from the 28,152 bank card transactions from the finance system that were made during the audit period and traced the cardholders' names, the last four digits of the bank cards' numbers, the transaction dates, the vendor names, the dollar amount of the transactions, and the transaction numbers to the 20 transactions listed on relevant bank statements. From the 28,152 transactions from the finance system, we identified a total population of 19,556 UMass Lowell bank card transactions that were made during our audit period.<sup>10</sup> We then verified that all cardholders relevant to this population of 19,556 UMass Lowell bank card transactions were UMass Lowell employees by tracing their names to a list of all UMass Lowell employees from HR/CMS.

To determine the reliability of the list of computer network users who had access to UMass Lowell's computer network, we obtained a list of the 2,071 computer network users who were able to access the computer network during our audit period. We inspected the list of 2,071 computer network users for hidden rows and columns, embedded data, and invisible content. From the 2,071 computer network users, we identified a population of 1,137 nonfaculty employees who were required to have cybersecurity awareness training during our audit period. To determine whether the list of computer network users was accurate and complete, we selected a sample of 20 computer network users from the population of 1,137 nonfaculty employees. We then verified the employment status for each computer network user in our sample by tracing their names to the list of all UMass Lowell employees from HR/CMS. Further, we tested certain security management and access controls over UMass Lowell's cybersecurity awareness

---

9. Embedded data is data within a Microsoft Excel worksheet that was added from another source and/or data that cannot be edited.

10. The UPST bank card manager provided us with a list of all UMass Dartmouth and UMass Lowell bank card transactions during the audit period, which amounted to 28,152 transactions. From those transactions, 19,556 were transactions made by UMass Lowell cardholders. The remaining 8,596 transactions were UMass Dartmouth transactions and not related to this audit.

training platform, and we reviewed a System and Organization Control 2 report<sup>11</sup> (which is called *A Type 2 Independent Service Auditor's Report on Controls Relevant to Security, Availability, and Confidentiality*) on UMass Lowell's cybersecurity awareness training platform.

Based on the results of the data reliability assessment procedures described above, we determined that the information obtained for our audit period was sufficiently reliable for the purposes of our audit.

---

11. A System and Organization Control report is a report on controls about a service organization's systems relevant to security, availability, processing integrity, confidentiality, or privacy issued by an independent contractor.

---

## DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

### 1. The University of Massachusetts Lowell's bank card transactions did not always comply with University of Massachusetts system policies and standards.

The University of Massachusetts (UMass) Lowell's bank card transactions did not always comply with UMass system policies and standards. We inspected 110 bank card transactions (89 transactions through U.S. Bank and 21 transactions through Citibank), totaling \$167,312, and found that some transactions were missing some or all supporting documents. Also, there were some instances where cardholders did not perform monthly bank statement reconciliations, either in a timely manner or at all. The following are details from our findings regarding these transactions.

#### Citibank Transactions

- Regarding documentation, 3 out of 21 transactions were missing a bank statement and a different 3 out of 21 transactions were missing both a bank statement and a receipt.
- Regarding state sales tax, 1 out of 21 transactions included this sales tax that was paid and never refunded to UMass Lowell by the vendor.

#### U.S. Bank Transactions

- Regarding documentation, 8 out of 89 transactions were missing a receipt, 3 out of 89 transactions were missing a bank statement, and 3 out of 89 transactions were missing both a bank statement and a receipt.
- Regarding state sales tax, 7 out of 89 transactions included this sales tax that was paid and never refunded to UMass Lowell by the vendor.
- Regarding travel, 7 out of 89 transactions related to out-of-state travel were missing a travel authorization number on either the bank statement, the receipt, or both.
- Regarding monthly reconciliations, the 89 transactions within our sample should have been included in a total of 87 requisitions. However, 5 requisitions were never created in the UMass system's online bank card transaction repository, while 48 were submitted after the allowable 30 days. The average number of days past due for these 48 requisitions was 112 days.
- Regarding missing information, 47 out of 89 transactions were missing information on their corresponding receipts.<sup>12</sup> Specifically,

---

12. Some of these 47 transactions had one or more instances of missing information on their corresponding receipts. In total, there were 62 instances of missing information.



- The vendor name was missing from 3 receipts.
- A description of the item purchased was missing from 6 receipts.
- A transaction date was missing from 5 receipts.
- The beginning and ending dates of the subscription period were missing on 3 receipts that were for subscription purchases.
- The last four digits of the bank card's number were missing from 15 receipts.
- A transparent business purpose was missing from 30 receipts.

If UMass Lowell does not reconcile and upload bank statements and supporting documents to the UMass system's online bank card transaction repository in a timely manner or at all, then UMass Lowell assumes a higher-than-acceptable risk of erroneous and potentially fraudulent bank card activity. If UMass Lowell pays taxes when they are not applicable, then it takes on an unnecessary tax burden that reduces funds available to support its mission. Furthermore, having incomplete documentation for bank card transactions on reconciliations results in a lack of transparency.

## Authoritative Guidance

UMass Lowell's cardholders are responsible for making allowable purchases, maintaining proper documentation, and completing timely reconciliations, according to Sections 2, 4, 11, 12, 15, and 21 of the UMass Bank Card Use Standard, which was updated on September 20, 2021. The standard states,

### 2. HOW IT WORKS . . .

*Each cardholder is responsible for downloading, reviewing, reconciling, and submitting their monthly statement to their supervisor . . . within 30 days of the statement issue date. . . .*

### 4. CARDHOLDER RESPONSIBILITIES . . .

*Cardholders are responsible for submitting all relevant receipts for all UMass Bank Card purchases. These receipts are to be submitted with the cardholder's monthly reconciliation. . . . If a receipt is lost, the cardholder must make every possible attempt to contact the vendor and obtain a copy. If a copy cannot be obtained, a Missing Receipt Affidavit may be filled out as the absolute last resort. . . .*

### 11. SALES TAX EXEMPTION . . .

*It is the responsibility of the cardholder to ensure that sales tax is not charged when the University is exempt when making a purchase with the UMass Bank Card. . . .*

*If a UMass Bank Card is charged tax, the cardholder is required to request a credit from the vendor as soon as the error is discovered. The cardholder is responsible for the follow-up until the vendor's credit is received.*

**12. RECEIPTS . . .**

*Receipts must include the following information:*

- *Vendor name*
- *Description of item purchased*
- *Transaction date . . .*
- *Beginning and expiration dates for subscriptions*
- *Proof that charge was billed to the UMass Bank Card (i.e., last 4 digits of card number)*
- *If not self-evident, a business purpose for the purchase. . . .*

**15. RECORD KEEPING**

*The Cardholder or their designee is responsible for obtaining a printed copy of the statement at the cycle end . . . and all receipts, packing slips, credit card slips, and invoices. . . .*

**21. TRAVEL RELATED INFORMATION . . .**

*If the travel required prior authorization . . . then travel authorization number must be referenced on the bank card statement and receipt.*

## **Reasons for Issue**

Regarding transactions that were missing some or all supporting documents, UMass Lowell stated that the UMass system's online bank card transaction repository is new to the UMass system. UMass Lowell management attributed the uploading of bank statements and supporting documents beyond the required timeframe, which we calculated to be an average of 112 days late, to the learning curve involved with using the new bank card transaction repository.

Regarding missing information, UMass Lowell management stated that the policy that calls for cardholders to write the travel authorization number on the bank statement and receipt(s) is not in practice throughout the entire UMass system. UMass system management also stated that the self-evidence of a transaction's business purpose is only required by the cardholder and supervisor, and further stated that the UMass Bank Card Use Standard does not officially document to whom the business purpose must be self-evident. After reviewing the supporting documents for the transactions in our

sample, we also noted that some of the missing information was caused by (1) the vendor's receipt not capturing certain details of the transaction, (2) a cardholder not capturing a full image of the receipt in a screenshot, or (3) the cardholder's submission of only the charge slip, which only displays a portion of the required information.

Regarding the state sales tax charges, UMass system management stated that some state sales tax charges were out of a cardholder's control, because of (1) the fact that some vendors would not accept UMass Lowell's sales tax-exempt status, especially vendors operating outside of Massachusetts, and (2) the inability to submit the Massachusetts tax exempt form to third-party vendors on platforms such as Amazon or eBay. Given these two issues, UMass system management stated that the small amount of sales tax charged is not always worth the time spent by the cardholder in trying to have the sales tax refunded.

## Recommendations

1. UMass Lowell should ensure that cardholders reconcile and upload all bank statements and supporting documents into the UMass system's online bank card transaction repository within 30 days of the bank statement date.
2. UMass Lowell should ensure that each bank card transaction receipt captures the full business purpose and that all required information is on the receipt. If this is not feasible within the requirements of the current standard, then the UMass system should update the UMass Bank Card Use Standard to reflect appropriate and feasible requirements.
3. UMass Lowell should ensure that state sales tax is not charged when bank card purchases are made by cardholders. If this is not feasible within the requirements of the current standard, then the UMass system should update the UMass Bank Card Use Standard to reflect appropriate and feasible requirements.
4. UMass Lowell should ensure that travel authorization numbers are referenced on the bank statement and receipt(s). If this is not feasible within the requirements of the current standard, then the UMass system should update the UMass Bank Card Use Standard to reflect appropriate and feasible requirements.

## Auditee's Response

1. *As part of its ongoing efforts to innovate and constantly improve efficiency and effectiveness of its operations, UMass is implementing a new University-wide expense system, which will improve the bank card reconciliation process. This new system will create a streamlined automated process where bank card transactions are imported and available daily for review. The new expense system includes monitoring controls to prompt timely review. As a result, the University will no longer utilize the online repository, and the Bank Card Standard will be updated to reflect new protocols.*

2. *The new expense system has a digital receipt capture feature that allows for them to be uploaded directly from a computer or mobile device. In addition, a mandatory field for business purpose is utilized in the new expense system. Cardholders are being trained to utilize these functions. As a result, the Bank Card Standard will be updated to reflect the new protocols. It is important to note that there were no fraudulent or inappropriate business purchases found during the audit and an explanation was provided for all transactions.*
3. *[UMass Lowell] understands the importance of minimizing its tax burden while also utilizing its resources efficiently. The total unrecovered sales tax found in this audit was approximately \$1,400. In addition, while the University is generally exempt from paying Massachusetts sales tax on purchases, that may not be the case in some other states. Each state's laws determine what organizations are exempt from its own sales tax. A reminder about the University's sales tax exemption will be communicated to cardholders and the Bank Card Standard will be reviewed and if necessary updated. . . .*
4. *To capture all trip related expenses in one place for the reviewer, travel authorization numbers were recorded in the finance system along with trip related bank card transactions instead of on a receipt or bank statement. The new expense system captures travel-related information, including, but not limited to, expenses, receipts and travel authorizations. As a result, the Bank Card Standard will be updated to reflect the new protocols.*

### **Auditor's Reply**

We commend the UMass system for implementing a new expense system for all UMass campuses and for ensuring that it will include a mandatory field for documenting the business purpose for each bank card transaction. We note that this new system is being implemented by the UMass system, and the weaknesses identified in this audit occurred independently at UMass Lowell. The new system may still be vulnerable to management and control weaknesses, such as the ones we identified, that occur at the level of each individual UMass campus.

We acknowledge that we ultimately determined the bank card transactions in our sample to be appropriate business purchases. However, this was not known by UMass Lowell. It is also possible that this issue occurred with transactions outside our sample. To determine whether the transactions in our sample were for appropriate business purchases, we requested that UMass Lowell management reach out to cardholders and their supervisors for clarification, because the necessary information was not captured on the receipts. Not capturing the full business purpose (when not self-evident) of each transaction on the receipt is a violation of the UMass Bank Card Use Standard and increases the risk that this information is not retained when employees leave UMass Lowell. It also increases the risk of fraud and financial loss if non-business-related transactions have occurred and not been detected by UMass Lowell.

We also acknowledge that the total dollar amount of unrecovered state sales tax found in our sample of transactions was approximately \$1,400. However, the UMass Bank Card Use Standard is clear in assigning responsibility to the cardholder for obtaining a refund in the event that state sales tax is charged and considered exempt, no matter how minimal the dollar amount. In its response, UMass Lowell mentioned that it is generally exempt from paying sales tax, depending on the state. However, out of the eight transactions in our sample that were charged sales tax, seven transactions were charged Massachusetts sales tax and were never refunded by the vendor. The one remaining transaction involved a vendor address within New York, which is a tax-exempt state, based on the information that the Office of the President of the UMass system posts on its website. Therefore, all eight transactions should have had their sales taxes refunded to UMass Lowell by the vendor. The fact that our sample revealed transactions with unrecovered sales taxes means that the total population of 19,556 bank card transactions likely contains other transactions with unrecovered sales taxes of varying amounts. We commend the UMass system for planning to issue a reminder about its sales tax exemption to cardholders and for reviewing and updating the UMass Bank Card Use Standard, as necessary.

We also acknowledge that the travel authorization numbers from our sample were recorded in the finance system instead of the bank statements and receipts. However, referencing the travel authorization number on the bank statements and receipts is required by the UMass Bank Card Use Standard. If the expectation is for staff members to record travel authorization numbers in the finance system, rather than on bank statements and receipts, then the UMass Bank Card Use Standard should be updated to reflect this. The UMass Bank Card Use Standard was updated at least twice (first on September 20, 2022, and then again on June 1, 2023) after our audit period, and it still requires that travel authorization numbers be referenced on bank statements and receipts. We commend the UMass system for planning to update the UMass Bank Card Use Standard to reflect the new protocols but note that the management and control weaknesses referenced in this audit occurred at the level of an individual university, which did not comply with policies. The changes in computer systems and policies at a central level may therefore not resolve these issues, as they must be addressed, in this instance, by UMass Lowell itself.

Based on its response, the UMass system is taking measures to address our concerns by implementing new systems and policies, but we urge UMass Lowell to fully implement our recommendations, as they relate to issues found at the level of the university, not the entire UMass system.

## **2. The University of Massachusetts Lowell's cybersecurity awareness training documentation was missing crucial information, and the university did not ensure that all nonfaculty employees completed cybersecurity awareness training.**

Regarding newly hired employees, while UMass Lowell had documentation confirming that 16 newly hired employees (out of a sample of 20 newly hired employees who were required to complete cybersecurity awareness training during the audit period) completed this training, there was no documentation that confirmed the dates on which these employees were assigned to or completed this training. For the remaining 4 newly hired employees, 2 were assigned training but did not complete it and the other 2 were neither assigned nor completed the training.

Regarding existing employees, while UMass Lowell had documentation confirming that 48 existing employees (out of a sample of 60 existing employees who were required to complete cybersecurity awareness training during the audit period) completed this training, there was no documentation that confirmed the dates on which these employees were assigned to or completed this training. The remaining 12 existing employees were assigned training but did not complete it.

We projected the test results for the completion of cybersecurity awareness trainings from our sample of 80 nonfaculty employees to the population of 1,137 nonfaculty employees during our audit period. Based on this, we are 95% confident that at least 125 nonfaculty employees did not complete cybersecurity awareness training.

If UMass Lowell does not educate all employees on their responsibility to protect its information assets by requiring cybersecurity awareness training, then UMass Lowell is exposed to a higher-than-acceptable risk of cybersecurity attacks, which could cause financial and/or reputational losses.

### **Authoritative Guidance**

According to Section V (Procedures) of UMass Lowell's "Security Awareness Policy IT-5-112,"

***Video Awareness Training*** — *The Information Security Office will work with appropriate constituent groups to identify appropriate personnel and their roles (PCI-DSS, PII, Data Steward, and General Staff) and will ensure that all personnel attend appropriate awareness training upon hire and at least annually thereafter.*

Cybersecurity awareness training records should be retained, according to the "Massachusetts Statewide Records Retention Schedule," effective June 2018 and revised July 2021, which states,

---

**E04-08: Employee Training and Certification Records . . .**

*Documents the training of staff in compliance with state laws or agency rules and regulations. Includes training program materials, session schedules, attendance reports, continuing education documentation, in-service documentation, certification lists and documents, and related correspondence.*

**E04-08 (a): If filed separately from personnel file**

*Retain 10 years.*

**E04-08 (b): If filed in personnel file**

*Retain as long as personnel file is kept.*

**Reasons for Issue**

According to UMass Lowell's chief information security officer, when UMass Lowell updated its cybersecurity awareness training platform, the certificate of completion feature<sup>13</sup> was not enabled, and UMass Lowell lost the ability to track the dates when a training was assigned and/or completed during our audit period. It also lost the ability to create and print training certificates. In addition, during the cybersecurity awareness training platform update process, digital training records older than six months were inadvertently lost.

**Recommendations**

1. UMass Lowell should configure its cybersecurity awareness training platform so that it has the ability to monitor the assignment and completion of the trainings.
2. UMass Lowell should ensure that its nonfaculty employees complete cybersecurity awareness training when they are hired and annually thereafter.
3. UMass Lowell should retain sufficient cybersecurity awareness training documentation.

**Auditee's Response**

1. & 2. *Cybersecurity awareness training is only one part of a highly sophisticated and comprehensive cybersecurity program deployed by the campus to detect and prevent threats to the campus' information technology infrastructure, assets and data. UMass Lowell Information Technology is working with Human Resources to implement a new employee learning management platform that will track the completion of cybersecurity awareness training.*

---

13. The certificate of completion feature has the ability to generate training data, such as the dates when the trainings are assigned and completed. This feature also allows UMass Lowell to create and print training certificates.

3. *UMass Lowell Information Technology will collect and retain all cybersecurity awareness training records.*

### **Auditor's Reply**

Based on its response, UMass Lowell is taking measures to address our concerns on this matter.