

OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

Official Audit Report – Issued May 2, 2024

University of Massachusetts Dartmouth

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



OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

May 2, 2024

Dr. Mark Fuller, Chancellor
University of Massachusetts Dartmouth
285 Old Westport Road
Dartmouth, MA 02747

Dear Dr. Fuller:

I am pleased to provide to you the results of the enclosed performance audit of the University of Massachusetts Dartmouth. 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 Dartmouth. 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

EXECUTIVE SUMMARY	1
OVERVIEW OF AUDITED ENTITY	3
AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY	6
DETAILED AUDIT FINDINGS WITH AUDITEE’S RESPONSE.....	13
1. The University of Massachusetts Dartmouth’s bank card transactions did not always comply with UMass system policies and standards.	13
2. The University of Massachusetts Dartmouth did not provide cybersecurity awareness training for any of its employees.....	18

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) Dartmouth for the period July 1, 2020 through December 31, 2021.

In this performance audit, we determined whether UMass Dartmouth 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 Dartmouth ensured that its employees completed cybersecurity awareness training in accordance with Section 1 of Control 14 (Security Awareness and Skills Training) of the Center for Internet Security’s¹ Critical Security Controls.²

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

Finding 1 Page 13	UMass Dartmouth’s bank card transactions did not always comply with UMass system policies and standards.
Recommendations Page 16	<ol style="list-style-type: none">1. UMass Dartmouth 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 Dartmouth 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 Dartmouth 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 Dartmouth 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.

-
1. According to its website, the Center for Internet Security is a nonprofit entity with the mission “to make the connected world a safer place by developing, validating, and promoting timely best practice solutions that help people, businesses, and governments protect themselves against pervasive cyber threats.”
 2. According to the Center for Internet Security’s website, the “Critical Security Controls . . . are a prescriptive, prioritized, and simplified set of best practices that you can use to strengthen your cybersecurity posture. Today, thousands of cybersecurity practitioners from around the world use the [Critical Security Controls] and/or contribute to their development via a community consensus process.”

Finding 2 Page <u>18</u>	UMass Dartmouth did not provide cybersecurity awareness training for any of its employees.
Recommendations Page <u>19</u>	<ol style="list-style-type: none">1. UMass Dartmouth should provide cybersecurity awareness training to all employees when they are hired and annually thereafter.2. UMass Dartmouth should establish and implement a cybersecurity awareness training component to its information security policy. This component should include documented procedures, monitoring controls, and record retention requirements.

OVERVIEW OF AUDITED ENTITY

The University of Massachusetts (UMass) Dartmouth 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 Dartmouth 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 285 Old Westport Road in Dartmouth, with satellite campuses in North Dartmouth, Fairhaven, and Fall River.

According to UMass Dartmouth's website,

As chief executive officer of the campus, the Chancellor provides leadership in all areas of campus life, from academics and student affairs to the advancement of the university and the region. The Chancellor is also responsible for maintaining relationships with the UMass Office of the President and the UMass Board of Trustees.

During fiscal year 2021, UMass Dartmouth had a student population of approximately 6,710, a faculty employee population of 443, and a nonfaculty employee population of 639. During fiscal year 2021, UMass Dartmouth had \$241,240,000 in revenue, which included \$95,942,000 in state appropriations, and \$240,186,000 in expenses.

According to UMass Dartmouth's website,

UMass Dartmouth distinguishes itself as a vibrant, public research university dedicated to engaged learning and innovative research resulting in personal and lifelong student success. The University serves as an intellectual catalyst for economic, social, and cultural transformation on a global, national, and regional scale.

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 Dartmouth 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 documents³ to UMass Dartmouth 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

3. 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.

UMass system's online bank card transaction repository.⁴ According to the UMass Bank Card Use Standard, the steps the cardholder must take include the following.

■ 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.

■ The cardholder then uploads the bank statement and any supporting documents to the requisition.

■ The cardholder submits their requisition to their UMass Dartmouth 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 297 UMass Dartmouth cardholders, whose spending on items and services totaled approximately \$1.4 million.

Cybersecurity Awareness Training

UMass Dartmouth uses Section 1 of Control 14 (Security Awareness and Skills Training) of the Center for Internet Security's Critical Security Controls as guidance for cybersecurity awareness training. This guidance recommends formalizing a cybersecurity awareness training program to educate an agency's workforce and conducting "training at hire and, at minimum, annually."

4. 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) Dartmouth 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 Dartmouth 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?	No; see Finding <u>1</u>
2. Did UMass Dartmouth ensure that its employees completed cybersecurity awareness training in accordance with Section 1 of Control 14 (Security Awareness and Skills Training) of the Center for Internet Security's Critical Security Controls?	No; see Finding <u>2</u>

To accomplish our audit objectives, we gained an understanding of the aspects of UMass Dartmouth'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 Dartmouth 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 Dartmouth 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 8,596 bank card transactions made during the audit period, totaling \$1,435,388, into the following five categories.

Category Number	Category Description	Number of Transactions	Total Dollar Value of Transactions
1	Top 10 Highest Dollar Value Transactions	10	\$ 41,754
2	Transactions with Shared Transaction Numbers*	306	77,625
3	Amazon, eBay, and PayPal	2,471	242,255
4	Food and Groceries	259	33,274
5	All Remaining Transactions**	5,550	1,040,480
Total		<u>8,596</u>	<u>\$ 1,435,388</u>

* Each UMass Dartmouth 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 Dartmouth’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.

The method we used to select our sample, which consisted of 110 transactions and totaled \$59,410, is as follows:

- From category one, we selected all 10 transactions, which totaled \$41,754.
- From category two, we judgmentally selected 10 transactions (out of 306 transactions), which totaled \$7,549.
- From categories three through five, we used a 95% confidence level,⁵ a 50% expected error rate,⁶ and a 22% desired precision range⁷ to determine that our sample should consist of, at a minimum,

5. 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.

6. 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.

7. 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.

85 transactions. We then increased the sample size to 90 transactions and used Audit Command Language software⁸ to randomly select the following:

- From category three, we selected 45 transactions (out of 2,471 transactions), which totaled \$3,171.
- From category four, we selected 5 transactions (out of 259 transactions), which totaled \$824.
- From category five, we selected 40 transactions (out of 5,550 transactions), which totaled \$6,112.

Our sample of 110 transactions included 26 transactions that were made using Citibank procurement cards and 84 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 Dartmouth management, we requested that UMass Dartmouth management provide us with hard copies of these documents. Once we received these documents, we recorded which documents were submitted to UMass Dartmouth management and which were missing.

To determine whether UMass Dartmouth 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, since 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

8. 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.

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., marketing software and access to online news websites), 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 Dartmouth 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 Dartmouth, 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 Dartmouth management to inquire about how the purchases related to the goals and mission of UMass Dartmouth.

To determine whether each of the 110 transactions in our sample required a travel authorization number—a reference number indicating 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 Dartmouth 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,⁹ 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 Dartmouth. 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.

9. 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 Dartmouth adhered to Section 1 of Control 14 of the Center for Internet Security's Critical Security Controls regarding cybersecurity awareness training, we asked members of UMass Dartmouth management who were responsible for cybersecurity awareness training whether UMass Dartmouth ensured that all employees received initial and annual cybersecurity awareness training during the audit period.

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 Dartmouth'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 and columns, embedded data,¹⁰ 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

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

to the 20 transactions listed on relevant bank statements. From the 28,152 transactions from the finance system, we identified a total population of 8,596 UMass Dartmouth bank card transactions that were made during our audit period.¹¹ We then verified that all cardholders relevant to this population of 8,596 UMass Dartmouth bank card transactions were UMass Dartmouth employees by tracing their names to a list of all UMass Dartmouth employees from HR/CMS.

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. 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, 8,596 were transactions made by UMass Dartmouth cardholders. The remaining 19,556 transactions were UMass Lowell transactions and not related to this audit.

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

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

The University of Massachusetts (UMass) Dartmouth's bank card transactions did not always comply with UMass system policies and standards. We inspected 110 bank card transactions (84 transactions through U.S. Bank and 26 transactions through Citibank), totaling \$59,410, 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, 4 out of 26 transactions were missing a bank statement.
- Regarding state sales tax, 1 out of 26 transactions included this sales tax that was paid and never refunded to UMass Dartmouth by the vendor.

U.S. Bank Transactions

- Regarding documentation, 2 out of 84 transactions were missing a receipt, 3 out of 84 transactions were missing a bank statement, and 2 out of 84 transactions were missing both a bank statement and a receipt.
- Regarding state sales tax, 1 out of 84 transactions included this sales tax that was paid and never refunded to UMass Dartmouth by the vendor.
- Regarding travel, 4 out of 84 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 84 transactions within our sample should have been included in a total of 80 requisitions. However, 9 requisitions were never created in the UMass system's online bank card transaction repository, while 34 were submitted after the allowable 30 days. The average number of days past due for these 34 requisitions was 153 days.
- Regarding missing information, 28 out of 84 transactions were missing information on their corresponding receipts.¹² Specifically,
 - The vendor name was missing from 3 receipts.

12. Some of these 28 transactions had one or more instances of missing information on their corresponding receipts. In total, there were 45 instances of missing information.

- A description of the item purchased was missing from 2 receipts.
- A transaction date was missing from 4 receipts.
- A transaction total was missing from 2 receipts.
- The last four digits of the bank card's number were missing from 17 receipts.
- A transparent business purpose was missing from 17 receipts.

If UMass Dartmouth 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 Dartmouth assumes a higher-than-acceptable risk of erroneous and potentially fraudulent bank card activity. If UMass Dartmouth 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 Dartmouth'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*
- *Transaction total . . .*
- *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 Dartmouth stated that the UMass system's online bank card transaction repository is new to the UMass system. UMass Dartmouth management attributed the uploading of bank statements and supporting documents beyond the required timeframe, which we calculated to be an average of 153 days late, to the learning curve involved with using the new bank card transaction repository.

Regarding missing information, UMass system 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 or (2) a cardholder not capturing a full image of the receipt in a screenshot.

Regarding the state sales tax charges, UMass system management stated that some state sales tax charges were out of a cardholder's control, because some vendors would not accept UMass Dartmouth's sales tax-exempt status, especially vendors operating outside of Massachusetts. Given this, 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

- UMass Dartmouth 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.
- UMass Dartmouth 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.
- UMass Dartmouth 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.
- UMass Dartmouth 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 Dartmouth] 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*

\$2. 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 Dartmouth. 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 Dartmouth. 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 Dartmouth 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 Dartmouth. It also increases the risk of fraud and financial loss if non-business-related transactions have occurred and not been detected by UMass Dartmouth.

We also acknowledge that the total dollar amount of unrecovered state sales tax found in our sample of transactions was approximately \$2. 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 Dartmouth mentioned that it is generally exempt from paying sales tax, depending on the state. However, the 2

transactions in our sample were charged Massachusetts sales tax and were never refunded by the vendor. The fact that our sample revealed transactions with unrecovered sales taxes means that the total population of 8,596 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 Dartmouth 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 Dartmouth 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 Dartmouth did not provide cybersecurity awareness training for any of its employees.

UMass Dartmouth did not provide required cybersecurity awareness training for newly hired employees or annually thereafter for existing employees. Specifically, UMass Dartmouth did not ensure that all 84 newly hired employees and 605 existing employees completed any cybersecurity awareness training.

If UMass Dartmouth does not educate all employees on their responsibility to protect its information assets by requiring cybersecurity awareness training, then UMass Dartmouth is exposed to a

higher-than-acceptable risk of cybersecurity attacks, which could cause financial and/or reputational losses.

Authoritative Guidance

According to UMass system management, UMass Dartmouth follows Section 1 of Control 14 (Security Awareness and Skills Training) of the Center for Internet Security's Critical Security Controls for the cybersecurity awareness training of their employees. This control states,

Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.

Reasons for Issue

UMass Dartmouth information technology management stated in an interview with us on May 22, 2023 that "cybersecurity awareness training fell on the backburner these past years due to a 20% staffing shortage." They also stated that the current UMass Dartmouth information security policy does not contain verbiage to enforce, monitor, or document completion of cybersecurity awareness training requirements for newly hired employees or annual training for existing employees.

Recommendations

- UMass Dartmouth should provide cybersecurity awareness training to all employees when they are hired and annually thereafter.
- UMass Dartmouth should establish and implement a cybersecurity awareness training component to its information security policy. This component should include documented procedures, monitoring controls, and record retention requirements.

Auditee's Response

1. *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. All employees took the mandatory cybersecurity awareness video training in April 2023 via our learning management system. All new employees are required to take the training as part of the on-boarding process. Annually, all employees will be required to take a refresher course and emails will be sent out with the link to the learning management system training site. Furthermore, management monitors whether employees have timely completed training. The training material will be reviewed periodically and if necessary, the material will be revised for any new and applicable authoritative guidelines.*

2. *UMass Dartmouth's Human Resource and Information Technology departments will develop and implement a Campus Cybersecurity Awareness Policy; once approved, it will be posted on the Campus website.*

Auditor's Reply

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