OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

Official Audit Report – Issued September 6, 2024

University of Massachusetts Chan Medical School

For the period July 1, 2021 through December 31, 2022

OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

September 6, 2024

Dr. Michael F. Collins, Chancellor
University of Massachusetts Chan Medical School
55 Lake Avenue North
Worcester, MA 01655

Dear Dr. Collins:

I am pleased to provide to you the results of the enclosed performance audit of the University of Massachusetts Chan Medical School. As is typically the case, this report details the audit objectives, scope, methodology, findings, and recommendations for the audit period, July 1, 2021 through December 31, 2022. 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 Chan Medical School. 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

LIST OF ABBREVIATIONS

Chan	Chan Medical School
HR/CMS	Human Resources Compensation Management System
UMass	University of Massachusetts
UPST	Unified Procurement Services Team

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) Chan Medical School (Chan) for the period July 1, 2021 through December 31, 2022.

In this performance audit, we determined whether UMass Chan executed all bank card purchases in accordance with Sections IV(A) and (B) within Appendix C of the "University of Massachusetts Business and Travel Expense Policy" (document T92-031); Articles I and II of the "University of Massachusetts Administrative Standards for Business and Travel Expense Policy"; and Sections 2, 4–8, 11, 12, 15, and 21 of the UMass Bank Card Use Standard. We also determined whether UMass Chan adhered to its "Privacy and Security Training Policy" regarding cybersecurity awareness.

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

Finding 1 **Page 15**	UMass Chan's bank card transactions did not always comply with UMass system policies and standards.
Effect	If UMass Chan 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 Chan assumes a higher-than-acceptable risk of erroneous and potentially fraudulent bank card activity. In addition, having incomplete documentation for bank card transactions on reconciliations results in a lack of transparency.
Recommendations **Page 17**	1. UMass Chan should ensure that travel authorization numbers are referenced on bank statements and receipts. 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. 2. UMass Chan 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 bank statement dates.
Finding 2 **Page 18**	UMass Chan did not ensure that workforce members completed cybersecurity awareness training in a timely manner.
Effect	If UMass Chan does not educate all workforce members on their responsibility to protect information assets by requiring cybersecurity awareness training, then UMass Chan is exposed to a higher-than-acceptable risk of cybersecurity attacks, which could cause financial and/or reputational losses.
Recommendation **Page 20**	UMass Chan should ensure that all workforce members who have access to its computer network complete cybersecurity awareness training in a timely manner, upon hire and annually thereafter.

OVERVIEW OF AUDITED ENTITY

The University of Massachusetts (UMass) Chan Medical School (Chan), formerly known as UMass Medical School, was established by the Commonwealth in July 1962. UMass Chan, which is located in Worcester, is one of five campuses (along with Amherst, Boston, Dartmouth, and Lowell) in the UMass system. The UMass system was established under Section 1 of Chapter 75 of the Massachusetts General Laws. A president oversees the UMass system, while individual chancellors oversee each campus. The president and a 22-member board of trustees provide governance to the UMass system.

UMass Chan is a member of the Massachusetts public higher education system, which consists of 15 community colleges, nine state universities, and the five UMass campuses. According to UMass Chan's website, it is "the commonwealth's first and only public academic health sciences center."

During fiscal year 2022, UMass Chan had a student population of approximately 1,246 and an employee population of 3,775. Also during fiscal year 2022, UMass Chan had $1,017,143,000 in revenue, which included $60,392,000 in state appropriations,[1] and $1,007,677,000 in expenses.

According to the UMass Chan Strategic Plan 2020–2025,

> *Our mission is to advance the health and wellness of our diverse communities throughout Massachusetts and across the world by leading and innovating in education, research, health care delivery and public service.*

The UMass Chan Strategic Plan 2020–2025 also lists the following as UMass Chan's strategic goals:

> *Education: Advance practice, learning and leading by engaging fully with our communities to be the destination of choice for learners interested in interprofessional, team-based care and biomedical entrepreneurship*
>
> *Basic Science Research: Enable the engine of discovery to generate groundbreaking scientific knowledge, with continued focus on areas of world-class strength*
>
> *Translational Research: Enhance innovation and increase impact by advancing the science of translation and channeling more discoveries into development and practice*
>
> *Community and Global Impact: Measurably improve the health and welfare of the residents of Massachusetts and the citizens of the world by investing in an enhanced social mission that engages*

1. Other sources of revenue included $675,740,000 in operating revenue (which included sources like grants, tuition, and fees) and $281,011,000 in nonoperating revenue.

community partners, advances health equity research and promotes public health interventions for the benefit of those greatest in need

Operational Excellence and Financial Stewardship: Establish models for outstanding support services, vibrant working environments and highly efficient infrastructure to propel UMass Chan to new heights

Diversity, Equity and Inclusion: Create more inclusive, equitable environments across the entirety of the medical school so that UMass Chan can better attract, support and advance diverse staff, faculty and learners

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

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 Chan 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."

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.

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[2] to UMass Chan 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.[3] 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.
    - Cardholders who are engaged in out-of-state travel must take specific steps. A UMass Chan cardholder needs to generate a travel authorization number for any out-of-state travel-related transactions. A travel authorization number is a reference number indicating that the travel was preapproved. This travel authorization number then needs to be marked on the bank statement and any receipt(s) that correspond to the out-of-state travel in question.
3. The cardholder submits their requisition to their UMass Chan supervisor for approval.[4] 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 the cardholder's supervisor approves it, at which time the bank card transaction repository timestamps the requisition again.

During the audit period, there were 553 UMass Chan cardholders, whose spending on goods and services totaled approximately $12.3 million. This figure encompasses the following data points:

- an average of $295 per bank card transaction;

2. 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.
3. 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."
4. Both the submission and approval of the requisition occur in the online bank card transaction repository.

- a total of 7,900 transactions that cost $25 or less;
- a total of 25 transactions that cost $7,500 or more; and
- a grand total of 41,848 transactions.

Cybersecurity Awareness Training

UMass Chan's "Privacy and Security Training Policy" states, "This policy affects all UMass Chan 'Workforce,' defined for this policy as faculty, staff, contingent workers, contractors and students engaged with all UMass Chan schools, departments, centers and business units."

UMass Chan requires all of its workforce members who receive UMass Chan computer network access to complete cybersecurity awareness training. Specifically, UMass Chan's "Privacy and Security Training Policy" states,

> *Initial training must be completed within fourteen (14) days after receiving access to UMass Chan networks or systems for all Workforce members. . . .*
>
> *Annual Security and Privacy training for all Workforce members must be completed within sixty (60) days.*

UMass Chan provides cybersecurity awareness training through a web-based, third-party platform. The cybersecurity awareness training platform tracks and records all activities and documentation (e.g., assignment status, automatic reminders, completion status, and training completion certificates) regarding cybersecurity awareness training for each workforce member.

According to the "Privacy and Security Training Policy" and UMass Chan officials, UMass Chan's Information Technology Department, using the cybersecurity awareness training platform, tracks and monitors the training completion status for each workforce member. For workforce members who do not complete cybersecurity awareness training within the specified timeframe, the "Privacy and Security Training Policy" states that the escalation process occurs as follows:

- *Initial training: . . .*
    - *If initial training is not completed after fourteen (14) days, users will receive a written reminder.*
    - *If the initial training has not been completed within thirty (30) days, the Workforce member's manager or supervisor will be notified. Escalation to Department Chairs / Business Unit Leaders may result.*

- *If initial training is still incomplete after sixty (60) days, Umass Chan Department Unit Heads and Senior Management will be made aware and disciplinary actions may result, including counseling, verbal warning, and/or suspension from or use of UMass Chan systems.*

- *Annual training: . . .*
- *If the user does not complete the training [within sixty (60) days], the following shall occur:*
    - *Sixty (60) days from receiving the training assignment, users will receive a written reminder to complete the training.*
    - *If the training has not been completed within ninety (90) days, the Workforce member's manager or supervisor will be notified. Escalation to Department Chairs/ Business Unit Leaders may result.*
    - *If training is still incomplete after one hundred twenty (120) days, UMass Chan Department Unit Heads and Senior Management will be made aware and disciplinary actions may result, including counseling, verbal warning, and/or suspension from or use of UMass Chan systems.*

According to UMass Chan officials, UMass Chan has an automated lockout control that suspends access to UMass Chan's computer network for any workforce member who does not complete the training after 60 days past the initial training assignment date and 120 days past the annual refresher training assignment date.

If a workforce member is locked out of UMass Chan's computer network system due to noncompliance with the cybersecurity awareness training policy, then that workforce member must contact the UMass Chan Information Technology Department to unlock their UMass Chan account. The workforce member then receives limited computer network access that only includes authorization to the cybersecurity awareness training platform so they can complete the outstanding training. Once the workforce member completes their outstanding training, UMass Chan's Information Technology Department manually reactivates that workforce member's access to UMass Chan's computer network.

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) Chan Medical School (Chan) for the period July 1, 2021 through December 31, 2022.

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 Chan execute all bank card purchases in accordance with Sections IV(A) and (B) within Appendix C of the "University of Massachusetts Business and Travel Expense Policy" (document T92-031); Articles I and II of the "University of Massachusetts Administrative Standards for Business and Travel Expense Policy"; and Sections 2, 4–8, 11, 12, 15, and 21 of the UMass Bank Card Use Standard?	**No; see Finding 1**
2. Did UMass Chan adhere to its "Privacy and Security Training Policy" regarding cybersecurity awareness training?	**Partially; see Finding 2**

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

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

Bank Card Purchases

To determine whether UMass Chan executed all bank card purchases in accordance with Sections IV(A) and (B) within Appendix C of the "University of Massachusetts Business and Travel Expense Policy" (document T92-031); Articles I and II of the "University of Massachusetts Administrative Standards for

Business and Travel Expense Policy"; and Sections 2, 4–8, 11, 12, 15, and 21 of the UMass Bank Card Use Standard, we performed the actions described below.

We distributed the total population of 41,848 bank card transactions made during the audit period, totaling $12,326,504, into the three categories described below.[5]

Category Number	Category Description	Number of Transactions	Total Dollar Value of Transactions
1	$7,500 or Higher	25	$ 232,541
2	Online (i.e., Amazon, eBay, PayPal), Food, and Grocery Vendors	8,118	1,370,060
3	All Remaining Transactions*	33,705	10,723,903
	Total	41,848	$ 12,326,504

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

The method we used to select our sample, which consisted of 128 bank card transactions totaling $281,771, is as follows:

- From category one, we selected all 25 transactions, which totaled $232,541.
- From categories two and three, we used a 95% confidence level,[6] a 50% expected error rate,[7] and a 20% desired precision range[8] to determine that our sample should consist of, at a minimum, 103 transactions. We then randomly selected the following:
  - From category two, we selected 20 transactions (out of 8,118 transactions), which totaled $10,102.
  - From category three, we selected 83 transactions (out of 33,705 transactions), which totaled $39,129.

See the following sections for actions we took with our sample of 128 transactions.

5. The average bank card transaction during the audit period was $295.
6. 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.
7. 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, based upon the implementation of the UPST system and understanding of controls gained in planning, we assume there are relatively frequent errors in the data the auditee provided to us.
8. 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. We chose a 20% desired precision range based on our understanding of the population of bank card transactions and the expected error rate of 50%.

Submission of Bank Card Transaction Documents

For each of the 128 transactions in our sample, we performed the actions described below.

To determine whether UMass Chan 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 128 transactions in our sample in the bank card transaction repository. We recorded the creation dates of the relevant requisitions. We then took screenshots of each bank statement and any supporting documents within the bank card transaction repository. If any of the transactions in our sample were missing bank statements or receipts, which were required to be submitted, the UPST member obtained those from the cardholders. Once 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.

See Finding 1 for information about the results of our testing regarding submissions of bank card transaction documents.

Information on Receipts and Bank Statements

For each of the 128 transactions in our sample, we performed the actions described below.

We inspected each receipt to ensure that it 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 number used to make the purchase. We obtained screenshots of each requisition and inspected them for cardholder and supervisor signatures.

To determine whether each receipt and/or purchase log related to each transaction in our sample 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 business purpose was not documented 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 Chan 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 transaction in our sample was related to the goals and mission of UMass Chan, we inspected the bank statements and supporting documents to identify the types of purchases. We noted whether the purchases had a documented business purpose and was approved by the cardholder's supervisor. We also met with UMass system and UMass Chan management to ask how the purchases related to the goals and mission of UMass Chan.

Additionally, we identified which transactions were travel-related by inspecting the supporting documents for vendor names and transaction descriptions related to travel (e.g., airlines, lodging, or car rental agencies). For out-of-state travel-related transactions in our sample, we inspected the supporting documents, confirming that each transaction was for out-of-state travel and was for a business-related purpose. We then inspected each travel-related receipt and bank statement for a travel authorization number, if applicable.

We identified which transactions were for subscriptions (e.g., marketing software or access to online news websites) by inspecting the receipts for descriptions of what was purchased. For those transactions in our sample that were for subscriptions, we inspected each receipt for subscription start date and end dates.

See Finding 1 for information about the results of our testing regarding information on bank statements and receipts.

Allowable Purchases

For each of the 128 transactions in our sample, we performed the actions described below.

To determine whether a transaction 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. We noted that no transactions in our sample were for foreign expenses.

To determine whether a transaction was for out-of-state travel, we inspected the relevant supporting documents (i.e., receipts and invoices) for vendor addresses that were out-of-state and for any notations that the transaction was for travel or travel-related meals. We also inspected screenshots of preapprovals for the transactions in our sample that were for out-of-state overnight travel.

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 the sales tax was refunded by the vendor to UMass Chan.

We noted no exceptions in our testing; therefore, we concluded that all 128 transactions were for allowable purchases.

Cybersecurity Awareness Training

To determine whether UMass Chan followed its "Privacy and Security Training Policy" regarding cybersecurity awareness training, we performed the actions described below.

We obtained a list of workforce members who were employed at some point during the audit period, which UMass Chan provided to us as a Microsoft Excel spreadsheet. According to UMass Chan officials, this list contained all UMass Chan workforce members who had the potential to access UMass Chan's computer network (meaning that the list included workforce members who did and did not have access to UMass Chan's computer network). UMass Chan management explained that they were unable to provide a list of only the workforce members who had access to UMass Chan's computer network because UMass Chan's human resources system was unable to generate reports with that level of detail. Therefore, this list of 7,932 UMass Chan workforce members who were employed at some point during the audit period was the only source available to identify a population of UMass Chan workforce members who were required to complete cybersecurity security awareness training during the audit period.

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

UMass Chan had a population of 7,932 workforce members who were employed at some point during the audit period (which included individuals whose employment with UMass Chan ended at some point during the audit period). We distributed these 7,932 workforce members into the following two categories: 1,972 workforce members who were hired during the audit period (i.e., newly hired workforce members) and were required to complete initial cybersecurity awareness training and 5,960 workforce members who were hired before the audit period (i.e., existing workforce members) and were required to complete annual refresher cybersecurity awareness training. We selected a random, statistical[10] sample of 60 newly hired workforce members from our population of 1,972 and another random, statistical sample of 60 existing workforce members from the population of 5,960, and, in both cases, used a 95% confidence level, a 0% expected error rate, and a 5% tolerable error rate.[11]

To determine whether UMass Chan ensured that workforce members from our two samples completed cybersecurity awareness training—the initial training for our sample of 60 newly hired workforce members and the annual refresher training for our sample of 60 existing workforce members—in a timely manner, we took the following actions with each sample. We obtained evidence (e.g., certification of completion) from UMass Chan's cybersecurity awareness training platform and inspected each assignment date and completion date recorded in the cybersecurity awareness training platform. In addition, for each of the workforce members in our samples whose employment with UMass Chan ended during the audit period (of which there were 12 newly hired workforce members and 12 existing workforce members), we obtained evidence (i.e., screenshots of users' UMass Chan employment status, which we obtained from UMass Chan's human resources system) showing the end date of each user's employment status with UMass Chan, which would also deactivate each user's access to UMass Chan's computer network.

See Finding 2 for information about the results of our testing regarding cybersecurity awareness training.

We used statistical sampling methods for testing; however, we did not project the results of our testing to the corresponding population(s).

10. Auditors use statistical sampling to select items for audit testing when a population is large (usually over 1,000) and contains similar items. Auditors generally use a statistics software program to choose a random sample when statistical sampling is used. The results of testing using statistical sampling, unlike those from judgmental sampling, can usually be used to make conclusions or projections about entire populations.
11. 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.

Data Reliability Assessment

Bank Card Purchases

To determine the reliability of the bank card transaction data, we interviewed UMass system officials who were knowledgeable about the data. We also tested the security management and access controls for UMass Chan'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 all 56,846 bank card transactions that were made during the audit period. The UPST bank card manager then provided these 56,846 bank card transactions to us in a Microsoft Excel spreadsheet. We ensured that the total number of 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,[12] and invisible content. We also inspected the bank card transaction data to see whether a transaction number appeared more than once within the data. Because we did see transaction numbers occur in the data more than once, we then tested whether these transaction numbers were shared transaction numbers[13] (which can occur because of acceptable business processes) or were duplicate transaction numbers (which should not occur). We did this by selecting a judgmental[14] sample of five transaction numbers that appeared more than once and verified that these five transaction numbers were not duplicated in the general ledger. Then, from the 56,846 bank card transactions, we removed any transactions with non-unique transaction numbers, resulting in a total population of 41,848 unique bank card transactions.

To determine the completeness of the population of 41,848 unique bank card transactions, we judgmentally selected a sample of 20 transactions listed on bank statements and compared them to the 41,848 unique 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 selected a random sample of 20 bank card transactions from the 41,848 unique bank card transactions from

12. Embedded data is data within a Microsoft Excel worksheet that was added from another source and/or data that cannot be edited.
13. Each UMass bank card transaction has a unique transaction number assigned to it by the bank during the transaction process. Transactions with shared transaction numbers can be attributed to various situations, such as splitting the cost of purchased items with multiple departments.
14. Auditors use judgmental sampling to select items for audit testing when a population is very small, the population items are not similar enough, or there are specific items in the population that the auditors want to review. Auditors use their knowledge and judgment to select the most appropriate sample. For example, an auditor might select items from areas of high risk. The results of testing using judgmental sampling cannot be used to make conclusions or projections about entire populations; however, they can be used to identify specific issues, risks, or weaknesses.

the finance system that were made during the audit period and traced the cardholders' names, the last four digits of the bank card numbers, the transaction dates, the vendor names, the dollar amounts of the transactions, and the transaction numbers to the 20 transactions listed on relevant bank statements. We then verified that all cardholders relevant to this population of 41,848 unique bank card transactions were UMass Chan employees by tracing their names to a list of individuals who were actively employed by UMass Chan during the audit period, which we generated independently from HR/CMS.

Cybersecurity Awareness Training

To determine the reliability of the list of 7,932 UMass Chan workforce members who were employed at some point during the audit period, we took the following actions. We conducted interviews with UMass Chan officials who were knowledgeable about the data. Also, during a remotely held meeting, we observed a UMass Chan information technology employee log into the cybersecurity awareness training platform and show us the cybersecurity awareness training process, starting with the assignment of the training to a workforce member and concluding with the workforce member's receipt of the training completion certificate.

We inspected the list of 7,932 UMass Chan workforce members for hidden rows and columns, embedded data, invisible content, and duplicate information. In addition, we selected a random sample of 20 workforce members from the list and verified their employment status with UMass Chan by tracing employee information—i.e., employee identification number, name, pay status,[15] department, job title, campus location, employee class,[16] start date, rehire date (if applicable), and termination date (if applicable)—to the employee information in the electronic personnel files maintained by the UMass Chan Human Resources Department. To test the completeness of the list of 7,932 workforce members, we compared this list to a list of individuals who were actively employed by UMass Chan during the audit period, which we generated independently from HR/CMS.

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

15. Pay status indicates an employee's current employment situation (e.g., active, terminated, or on leave with pay).
16. Employee class indicates an employee's classification (e.g., dual-employed physician, staff member, or faculty member).

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

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

The University of Massachusetts (UMass) Chan Medical School's (Chan's) bank card transactions did not always comply with UMass system policies and standards. We inspected 128 bank card transactions made during the audit period, totaling $281,771, and found that some transactions were missing some or all supporting documents. There were also 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:

- Regarding travel-related documentation, 9 transactions out of our sample of 128 required a travel authorization number because they were related to out-of-state travel. However, 6 out-of-state travel-related transactions out of these 9 were missing a travel authorization number on either the bank statement, the receipt, or both.
- Regarding monthly reconciliations, note that the 128 transactions within our sample were filed in a total of 127 requisitions.
    - Of the 127 requisitions related to our sample of transactions, 2 requisitions were never created in the UMass system's online bank card transaction repository, while 42 were submitted after the allowable 30 days. The median number of days past due for these 42 requisitions was 22.5 days.
    - Regarding signatures needed for requisitions, 1 requisition out of 127 was missing a supervisor's approval signature.

If UMass Chan 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 Chan assumes a higher-than-acceptable risk of erroneous and potentially fraudulent bank card activity. In addition, having incomplete documentation for bank card transactions on reconciliations results in a lack of transparency.

Authoritative Guidance

UMass Chan's cardholders are responsible for making allowable purchases, maintaining proper documentation, and completing timely reconciliations, according to Sections 2, 4, 15, and 21 of the UMass Bank Card Use Standard. This standard states,

2. *HOW IT WORKS. . . .*

   Purchases are charged to the cardholder's department and each cardholder is responsible for downloading, reviewing, reconciling, and submitting their monthly statement to their supervisor for approval and signature within 30 days of the statement issue date. . . .

4. *CARDHOLDER RESPONSIBLITIES. . . .*

   Cardholders are responsible for submitting all required receipts for all UMass Bank Card purchases. These receipts are to be submitted with the cardholder's monthly reconciliation and will be subject to review and audit. . . .

   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 Form may be filled out as the absolute last resort. . . .

15. *RECORD KEEPING. . . .*

    All card statements are required to be signed by the cardholder and their supervisor. . . .

    Monthly statements and all required supporting documentation shall be submitted using the [the UMass system's Online Bank Card Transaction Repository] form. . . .

21. *TRAVEL RELATED INFORMATION. . . .*

    1. *If the travel required prior authorization (see UMass Business and Travel Policy), then travel authorization number must be referenced on the bank card statement and receipt.*

    2. *Receipts—Original receipts for UMass Bank Card transactions must be submitted with the UMass Bank Card Bank Statement. The only exception to this is for individual receipts under $25.00 while on travel status (Parking, Tolls, Taxi, etc. . . .). In order to capture all relevant information associated with a trip, UMass Bank Card users must also scan and attach the UMass Bank Card receipts to the online expense report along with any receipts for reimbursable expenses. In addition, hotel bills, airfare or any other UMass Bank Card charges related to the trip must be entered on the expense report. "Paid via ProCard" must be selected for payment type and "UMass Bank Card" must be selected for billing type. In circumstances where a traveler is inadvertently reimbursed on a UMass Bank Card receipt, the reimbursement must be returned to the University within 30 days of discovering the error.*

Reasons for Issue

Regarding missing travel-related information, UMass Chan management stated that the missing travel authorization number on the bank statement and receipt(s) was an oversight.

Regarding the 2 requisitions that were never created and the 42 that were submitted late, UMass Chan management told us that this was an oversight. UMass Chan management said that it was unclear

whether it was because someone assumed that it had already been uploaded or simply forgot to do so. They were uncertain about the exact reason(s) behind the failure to upload the documentation.

Regarding the requisition that was missing a supervisor's approval signature, UMass system officials acknowledged that this requisition was routed incorrectly; however, they could not explain why.

Recommendations

1. UMass Chan should ensure that travel authorization numbers are referenced on bank statements and receipts. 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.
2. UMass Chan 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 bank statement dates.

Auditee's Response

All nine travel authorizations cited were filed and approved, and all the travel authorization numbers were recorded in the finance system along with trip related bank card transactions. As part of its ongoing efforts to innovate and improve efficiency and effectiveness of its operations, UMass has implemented a new University-wide expense system that captures travel-related information, including, but not limited to, expenses, receipts and travel authorizations. As a result, the Bank Card Standard is being updated to reflect the new protocols.

The two cited reconciliations were manually approved and supporting documentation was maintained outside of the repository and provided to the auditors.

Furthermore, the new expense system improves the bank card reconciliation process and allows for a streamlined and 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 no longer utilizes the online repository, and the Bank Card Standard is being updated to reflect new protocols.

Auditor's Reply

We acknowledge that the travel authorization numbers from our sample were recorded in the finance system instead of on 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 once during the audit period (on September 20,

2022) and then again after the audit period (on June 1, 2023), and it still requires that travel authorization numbers be referenced on bank statements and receipts.

We also acknowledge that the two reconciliations referenced above were manually approved and that the corresponding supporting documentation provided to us was maintained outside of the UMass system's online bank card transaction repository. However, according to Section 15 (Record Keeping) of the UMass Bank Card Use Standard, this supporting documentation should have been submitted using the UMass system's online bank card transaction repository. Additionally, because this supporting documentation was maintained outside of the online bank card transaction repository, we were unable to determine the timeliness of the workflow for these two reconciliations.

We commend the UMass system for planning to update the UMass Bank Card Use Standard for all UMass campuses and for implementing a new expense system for all UMass campuses. However, while these changes will be made at the central level, the weaknesses referenced in this audit occurred on an individual-campus level. Therefore, the updates may not resolve these issues, as they must be addressed, in this instance, by UMass Chan itself. We strongly encourage UMass Chan to fully implement our recommendations regarding these matters.

2. The University of Massachusetts Chan Medical School did not ensure that workforce members completed cybersecurity awareness training in a timely manner.

UMass Chan did not ensure that workforce members completed cybersecurity awareness training in a timely manner. Regarding the initial cybersecurity awareness training, for 14 newly hired workforce members out of our sample of 60, we found the following:[17]

- Out of our sample of newly hired workforce members, 11 completed the training outside of the allotted timeframe of 14 days. Based on the assignment date for each of these workforce members, the median number of days past due for these trainings was 21 days beyond the allotted 14 days.
- Out of our sample of newly hired workforce members, 3 never completed their initial cybersecurity awareness training.[18]

17. Out of our sample of newly hired workforce members, 13 never received access to the UMass Chan computer network and, therefore, were never assigned to the cybersecurity awareness training.
18. During our audit, UMass Chan provided evidence that 2 of these workforce members completed their annual refresher training during the audit period (but not their initial training), and the remaining workforce member completed annual refresher training after the end of the audit period.

Regarding the annual refresher cybersecurity awareness training, from our sample of 60 existing workforce members, we found the following.

- For the 2021 annual refresher cybersecurity awareness training assignment, while 34 workforce members completed the training in a timely manner, we found the following:[19]
    - Out of our sample of existing workforce members, 8 completed the training outside of the allotted timeframe of 60 days. Based on the assignment date for each of these workforce members, the median number of days past due for these trainings was 60 days beyond the allotted 60 days.
    - Out of our sample of existing workforce members, 1 never completed the training.
- For the 2022 annual refresher cybersecurity awareness training assignment, while 28 workforce members completed the training in a timely manner, we found the following:[20]
    - Out of our sample of existing workforce members, 18 completed the training outside of the allotted timeframe of 60 days. Based on the assignment date for each of these workforce members, the median number of days past due for these trainings was 48.5 days beyond the allotted 60 days.

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

Authoritative Guidance

According to UMass Chan's "Privacy and Security Training Policy,"

> *All UMass Chan faculty, staff, contingent workers, contractors and students in its schools, departments, centers and business units are required to complete privacy and information security training. . . .*
>
> *Initial training must be completed within fourteen (14) days after receiving access to UMass Chan networks or systems for all Workforce members. . . .*
>
> *Annual Security and Privacy training for all Workforce members must be completed within sixty (60) days.*

19. Out of our sample of existing workforce members, 17 never received access to the UMass Chan computer network and, therefore, were never assigned to the cybersecurity awareness training.
20. Out of our sample of existing workforce members, 14 never received access to the UMass Chan computer network and, therefore, were never assigned to the cybersecurity awareness training.

Reasons for Issue

UMass Chan officials told us that some workforce members were never assigned access to the UMass Chan computer network because these employees did not complete the necessary steps to receive this access. As for the other workforce members, UMass Chan officials could not provide an explanation as to why these workforce members did not complete the required cybersecurity awareness training, either in a timely manner or at all.

Recommendation

UMass Chan should ensure that all workforce members who have access to its computer network complete cybersecurity awareness training in a timely manner, upon hire and annually thereafter.

Auditee's Response

UMass Chan has implemented a mature and effective Information Security and Privacy Training Program dedicated to educating our students, faculty, and workforce on how to recognize and respond to cybersecurity threats. As reflected in a nearly 100% completion rate, we are focused on effectively applying this critical security control and are committed to the program's continuous improvement. Awareness training is only one part of a highly sophisticated and comprehensive defense-in-depth cybersecurity framework deployed by the campus to detect and prevent threats to the campus' information technology infrastructure, assets and data. It is important to note that the individuals who were not assigned training was done so in line with UMass Chan policy because they never received access to the UMass Chan network and, as such, posed no security risk. Furthermore, the few individuals who did not complete cybersecurity awareness training have since either done so or left UMass Chan.

Auditor's Reply

We acknowledge that the workforce members noted in footnotes 17, 19, and 20 were not assigned cybersecurity awareness training because they never received access to the UMass Chan computer network, which is in line with UMass Chan policy. We included these footnotes because these workforce members appeared in our sample, which was selected from a list—provided to us by UMass Chan officials—of workforce members who were employed at some point during the audit period. According to UMass Chan officials, they provided us with this list—as opposed to a list of only the workforce members who had access to UMass Chan's computer network—because they were unable to provide the latter. (See "Cybersecurity Awareness Training" in the Audit Objectives, Scope, and Methodology section of this report for more information.) Nevertheless, of the workforce members in our sample who did receive access to the UMass Chan computer network, we identified 37 workforce members (11 newly

hired and 26 existing workforce members) who completed the cybersecurity awareness training late (both the initial and the annual refresher trainings), 3 newly hired workforce members who never completed the initial training, and 1 existing workforce member who never completed the 2021 annual refresher training. It is also possible that workforce members outside of our sample completed their training late or did not complete their training at all.

In its response, UMass Chan states that it "has implemented a mature and effective Information Security and Privacy Training Program . . . to recognize and respond to cybersecurity threats," but such a program requires timely cybersecurity awareness training for workforce members upon hire and annually thereafter. Such a program also requires continual monitoring by management if it is to be an effective program that protects UMass Chan's systems and data. Therefore, we strongly encourage UMass Chan to implement our recommendation regarding this matter.