OFFICE OF THE COMPTROLLER

ONE ASHBURTON PLACE, 9TH FLOOR
BOSTON, MASSACHUSETTS 02108
(617) 727-5000
MACOMPTROLLER.ORG

ELECTRONIC PAYMENTS DATA SECURITY

Effective: August 1, 2024
Last Updated: February 24, 2025

Executive Summary

This policy is jointly issued by the Office of the Comptroller (CTR) and the Executive Office of Technology and Security Services (EOTSS). CTR is required to implement a state accounting system and issue instructions for accounting practices, including payments, pursuant M.G.L. c. 7A, §§ 7, 8, and 9. Accordingly, this policy identifies minimum data security compliance requirements related to electronic payments and revenue received by departments. Also, this policy outlines requirements and best practices to comply with the statutes and regulations that mandate the protection of any confidential or personally identifiable information (PII) that is accepted, stored, processed, or transmitted by departments, including customer information related to fiscal transactions and payments.

Policy

This policy applies to Commonwealth departments legislatively authorized to collect taxes, revenues, fees, fines, and other funds. Multiple electronic payment acceptance options are available, including but not limited to credit cards, debit cards, Automated Clearing House (ACH), Electronic Funds Transfer (EFT), Interactive Voice Response (IVR), kiosk, web, point-of-sale, and mobile payments.

All Commonwealth Departments that currently accept credit or debit card payments are required to validate compliance with data security standards set by the PCI Security Standards Council. Compliance with these standards are enforced by the payment card brands for each merchant level, which depends upon the volume of transactions. Departments accepting revenues through an electronic payment mechanism must also comply with applicable standards and policies for revenue collection, the method of collection, and the protection of financial data as required under M.G.L. 93H and M.G.L. 93I, and the EOTSS Enterprise Information Security Policies and Standards.

Departments are required to protect PII and other confidential information stored, processed, or transmitted to support fiscal transactions, including the intake of payments, in accordance with security standards published by CTR and EOTSS. Departments will be asked to certify their compliance with this policy as part of CTR's annual Internal Controls Certification.

CTR has authority to review any proposed modification to the electronic collection of revenue. Therefore, departments must notify CTR's Non-Tax Revenue Team at eRev@mass.gov prior to any procurement or

executed change to the electronic collection of revenue. CTR reserves the right to direct a department to suspend electronic payment collections until CTR's review is completed.

Statewide Contract for Payment Data and Payment Card Industry Compliance Services

Departments accepting electronic payments should use the existing Statewide Contract for Payment Data and PCI Compliance Services. For more information about the Statewide Contract for Payment Data and PCI Compliance Services, please refer to the contract user guide.

The Payment Data and PCI Compliance Services Statewide Contract lists pre-qualified QSAs and other vendors that provide compliance audits, quality assurance reviews, and testing for PCI compliance, to protect personally identifiable information and other sensitive data.

Payment Card Industry Data Security Standard (PCI-DSS) for Acceptance of Credit and Debit Cards

All departments that currently accept credit or debit card payments are considered "merchants" or "sub-merchants" and are required to comply with the Payment Card Industry Data Security Standards (PCI-DSS) as a condition of statewide contracts PRF81, PRF82, and PRF84, and card brand rules. As a universal payment card industry requirement, departments must validate PCI-DSS set by the PCI Council regardless of whether they utilize the statewide contracts.

Therefore, any entity that accepts credit and debit cards must ensure sufficient funding to maintain continued compliance, including applicable assessments and penetration testing, remediate any condition to achieve compliance, and support continued vigilance in data security compliance. Compliance with these standards is enforced by the payment card brands. Departments must complete the appropriate Self-Assessment Questionnaire (SAQ)/Report on Compliance (ROC) annually and keep it on file at the ready if requested by the payment solutions or payment processing vendors. PCI Data Security Standards and related resources can be found at pcistandards.org.

Data Security for Other types of Electronic Payments Acceptance such as ACH - Commercially Reasonable Standards

Any entity accepting payments, whether or not deemed Commonwealth payments or recorded on MMARS, through collection options other than credit and debit cards, must seek and maintain sufficient funding to ensure compliance in adherence with revenue collection and data security standards published by CTR and EOTSS. Payment collection options, other than credit or debit cards include ACH, electronic checks, EFT, direct account debit, through any channel such as IVR, kiosk, web, point-of-sale and mobile devices, including but not limited to fees, fines, charges, tuition or tax payments, local or trust funds, interest or penalties, and any fiduciary funds Note that revenue collection and data security protocols are routinely audited as part of IT, operational, and federal grant audits.

Payment Data Security Maintenance Obligations

Departments should identify resources and funding to support ongoing data security compliance, including:

1. Training

Departments should train existing staff not less than annually on data security responsibilities. Departments should train new staff on these requirements before granting access to any PII, or before they may process payments.

2. Internal Controls

Under Chapter 647 of the Acts of 1989, the Comptroller is responsible for developing internal control guidelines for Commonwealth departments. Departments must develop and enforce rigorous internal controls to ensure the protection of any PII (e.g., customer cardholder or banking data) that is accepted, processed, stored, or transmitted related to fiscal transactions, to prevent compromise and/or breach. PCI and electronic payments data security goals and controls should be added to the department's Internal Control Plan and system of internal controls. Please visit macomptroller.org/internal-controls for more information and resources.

3. Initial and on-going data security compliance reviews.

As data breaches present a significant financial risk, initial baseline and ongoing data security compliance reviews as described in this policy are a necessary operational responsibility. Data security best practices must be accounted for in the department's annual budget. If the department accepts PII as part of operations, transactions, or the acceptance of payments. The department should evaluate any increased risk associated with implementing electronic payments and appropriate controls as part of its annual data security reviews.

4. Re-evaluations of material changes.

A department merchant or sub-merchant must evaluate data security compliance whenever the payment environment changes materially including, but not limited to, business and payment applications and systems, payment solutions, third party systems, processors, hardware and devices, software, or protocols, to ensure sufficient security of payment data and PII.

Data Breach Notice Responsibilities

In the event of a data breach by the department or a third-party processor, departments are required under M.G.L. c. 93H and 201 CMR 17.00 to provide proper notice of the breach to the Office of Consumer Affairs and Business Regulation, the Office of the Attorney General, and individuals whose personal information has been compromised. More information about data breach obligations under can be found on mass.gov/data-breaches and macomptroller.org/ctr-cyber/cyber-incidents. Departments must notify CTR and the Executive Office for Administration and Finance (A&F) of any budget deficiency or accounting issues related to their cost of compliance with these obligations.

Because departments record revenues in the Commonwealth's enterprise systems, to ensure these systems are protected, any incident involving a department or third-party processor that involves unauthorized data access, a data breach, or cyber incident must be communicated immediately to CTR (CTREmergencyNotification@mass.gov) and EOTSS (EOTSS-soc@mass.gov). CTR and EOTSS will assess risks to the enterprise systems and assist departments with internal controls and remediation.

Contact the Following with Questions Pertaining to this Policy

CTR Solution Desk	**(617) 973-2468**	comptroller.info@mass.gov