Commonwealth of

Massachusetts

Information Technology Division One Ashburton Place 8th Floor Boston, MA 02108		Office of the Comptroller One Ashburton Place 9th Floor Boston, MA 02108

MMARS Policy: Non-Tax Revenue
Issue Date: June 6, 2013
Date Last Revised: June 6, 2013

Payment Collection Data Security Policy

Executive Summary

This policy is jointly issued by the Office of the Comptroller (CTR) and the Information Technology Division (ITD) to identify minimum data security compliance requirements related to the collection of payments and the associated protection of personally identifiable information (PII) to prevent data breaches by all state Departments in all branches of state government. Departments legislatively authorized to collect money, revenues, fees, charges and other funds have multiple payments collection options, including electronic payment options and channels, including but not limited to credit cards, debit cards, Automated Clearing House (ACH) (electronic checks and direct account debit), Interactive Voice Response (IVR), web, point-of-sale and mobile devices. This policy outlines the state finance law and data collection security responsibilities Departments must maintain in connection with any PII collected or transmitted to support fiscal transactions, including the collection of money and electronic payments.

Acceptance of electronic payments provides administrative efficiencies by reducing the amount of cash and checks handled by Departments, but also increases data security risks because personally identifiable information (PII) such as bank account numbers, credit and debit card numbers, individual's names and other data are handled by individuals and systems and transmitted through electronic channels to complete the electronic transaction,

increasing the risk of a data breach or other unauthorized access, compromise, theft, loss or misuse of PII.

Departments are subject to a variety of state and federal statutes, regulations and policies that mandate the protection and non-disclosure of personal or confidential information including customer information related to fiscal transactions and accepting payments. (See G.L. c. 93H and G.L. c. 93I, Executive Order 504 (Executive Departments) and the Information Technology Division guidelines for Protection of Sensitive Information: http://www.macomptroller.info/comptroller/docs/forms/federal-grants/notice-of-application-of-a-federal-grant.doc and Information Security Policy: http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/security-policies-and-standards/information-security-policy.html.

Departments must take steps consistent with industry standards to ensure that the security and confidentiality of personally identifiable customer information (PII) is protected against anticipated threats or hazards to the security or integrity of such information and against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any customer.

Policy

The Comptroller has broad authority to prescribe accounting rules and instructions for all Departments and the appropriate use of the state accounting system. Pursuant to G.L. c. 7A, § 7, G.L. c. 7A, § 8, G.L. c. 7A, § 9 and G.L. c. 29, § 31, the Comptroller is required to implement a state accounting system (including a centralized payroll system) and issue instructions for accounting practices to be used by all Commonwealth entities for supplies, materials, assets, liabilities, equity, debt, encumbrances, expenditures, payments, expenses and obligations of all Commonwealth funds and accounts, including payroll, unless specifically exempted by general or special law. The Comptroller has full authority to prescribe, regulate and make changes in the method of keeping and rendering accounts and is authorized to direct Departments to implement changes in their systems to meet these statewide standards.

As a condition of this Policy, state law and to support fiscal responsibility, Departments must ensure that sufficient funds are maintained and set aside for initial and ongoing data security compliance responsibilities to protect PII and other confidential information stored, processed or transmitted to support fiscal transactions, including the collection of payments.

The Office of the Comptroller (CTR) administers a Data Security Audits Statewide Contract to assist with data security compliance to be used by any Department in any branch of state government storing, processing or transmitting PII and any Department accepting money irrespective of whether the Commonwealth Department is recording that money in the state accounting system MMARS or in a fiduciary capacity. Departments are required to certify as part of the annual Internal Control Questionnaire (ICQ) submission, compliance with data security requirements in connection with any PII collected or transmitted to support fiscal transactions, including the collection of money through electronic payments.

Payment Card Industry Council Data Security Standards for Acceptance of Credit and Debit Cards

All Departments that currently accept credit or debit card payments are considered "merchants" and are required to validate data security compliance. Compliance standards are set by the Payment Card Industry Council and compliance is enforced by the payment card brands for each merchant level, which depends upon the volume of transactions.

> *The Payment Card Industry Data Security Standard (PCI-DSS) secures cardholder data that is stored, processed or transmitted by merchants and other organizations. The standard is managed by the PCI Security Standards Council (PCI SSC) and its founders, the global payment brands: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.*
>
> *The PCI Data Security Standard and supporting documents represent a common set of industry tools and measurements to help ensure the safe handling of sensitive information. The standard provides an actionable framework for developing a robust account data security process - including preventing, detecting and reacting to security incidents. To reduce the risk of compromise and mitigate its impacts if it does occur, it is important that all entities storing, processing, or transmitting cardholder data be compliant.*
> (https://www.pcisecuritystandards.org/security_standards/index.php)

Any Department (in any branch of government) that accepts credit or debit cards is required to comply with the merchant requirements published by the Payment Card Industry Council in addition to any other state or federal laws, regulations or policies related to the storing, processing or transmitting of cardholder data which is considered PII. Depending on the Department's merchant level and volume of transactions, a Department may be required to complete a PCI-DSS Self-Assessment Questionnaire (SAQ) or a Report on Compliance (ROC) and file with their merchant bank, conduct quarterly vulnerability scans, penetration tests and facilitate periodic validation of Payment Card Industry Data Security Standards compliance (PCI-DSS).

PCI-DSS compliance is mandatory and a condition of acceptance of credit and debit cards. Under the Statewide Contract for Electronic Payments (ePay), the Commonwealth processing contractors and merchant banks provide services under the ePay Statewide Contract under the condition that Department merchants maintain PCI-DSS compliance. Therefore, it is a mandatory obligation for any Department merchant accepting credit and debit cards to ensure sufficient funding to maintain continued compliance, to remediate any condition to maintain compliance and to maintain continued vigilance in data security compliance.

Data Security Compliance Policy for Acceptance of Credit and Debit Cards (Validated Merchant Compliance)

Any Department merchant accepting credit/debit cards for any payments, for any purpose and from any source (including but not limited to fees, fines, charges, tuition or tax payments, local or trust funds, interest or penalties, and any fiduciary funds whether or not deemed Commonwealth payments or recorded on the Massachusetts Management and Accounting System "MMARS") is required to seek and maintain sufficient funding to ensure compliance with the following:

1. The Payment Card Industry Council Data Security Standards (PCI-DSS) for the applicable merchant level of transactions (https://www.pcisecuritystandards.org/security_standards/index.php).
    a. Independent validations of compliance by a Qualified Security Assessor (QSA) approved on the CTR Data Security Audits Statewide Contract, and
    b. Quarterly network scans and annual penetration tests by an Approved Scanning Vendor (ASV) on the Data Security Audits Statewide Contract if required.
2. The completion of at least **one initial independent validation** of data security compliance for the applicable merchant level under the PCI-DSS standards by a Qualified Security Assessor (QSA) approved under the CTR Data Security Audits Statewide Contract.
    a. **Application of independent "initial" validation**. This requirement applies to any Department in any Branch of state government accepting credit or debit cards for payments, even if under the PCI-DSS standards the merchant level does not require an independent validation or the merchant bank requires no formal documentation. The purpose of this independent

validation is to document data security due diligence and to document a data security compliance baseline for PCI-DSS standards for ongoing compliance and annual budgeting purposes. Independent "initial" validations of compliance conducted between 2010-2013 by an authorized Qualified Security Assessor (QSA) may be acceptable if the payment card environment, software and payment applications for the Department merchant have not materially changed.

b. **Scope of independent "initial" validation**. An independent data security compliance validation must be made by a Qualified Security Assessor (QSA) approved on the CTR Data Security Audits Statewide Contract of all payment collection methods including but not limited to payment applications, devices or channels, including but not limited to mail, cashier window, point of sale, telephone, web application, Interactive Voice Response (IVR) or mechanism, and mobile device payments. The Payment Card Industry Data Security Council requires the use of secure payment applications and maintains Payment Application Data Security Standards (PA-DSS) and a list of Validated Payment Applications. The independent validation ensures that the payment application complies with the Payment Application Data Security Standard if not already listed as a Validated Payment Application. New e-commerce implementations under the Comptroller E-Pay Statewide Contract are validated during the project development process. Payment collection methods must also be validated for state finance law compliance purposes by the Office of the Comptroller prior to implementation.

c. **Use of Internal Security Assessors (ISA)**. Department merchants whose employees have been trained, tested, qualified and attested as authorized Payment Card Industry Council Internal Security Assessors (ISA) may **not** conduct the "initial" validation of Payment Card Industry Data Security standards. This policy requires the initial validation to be conducted by an "independent" Qualified Security Assessor (QSA) approved on the CTR Data Security Audits Statewide Contract, even if the merchant level does not require an independent validation. Once the initial validation is completed, the Internal Security Assessor employees of the Department may conduct ongoing security audits but may not conduct special functions or QSA assessments.

Data Security Policy for Acceptance of Other types of Electronic Payments such as ACH (Validated Commercially Reasonable Standards)

Any Department accepting payments through collection options ***OTHER than credit and debit cards,*** such as Automated Clearing House (ACH), electronic checks, direct account debit, Interactive Voice Response (IVR), web, point-of-sale and mobile devices, for any payments, for any purpose and from any source (including but not limited to fees, fines, charges, tuition or tax payments, local or trust funds, interest or penalties, and any fiduciary funds whether or not deemed Commonwealth payments or recorded on the Massachusetts Management and Accounting System "MMARS") is required to seek and maintain sufficient funding to ensure compliance with the following:

1. The completion of at least **one initial independent validation** of commercially reasonable data security standards compliance for the storing, processing and transmitting of customer payment PII by a Qualified Security Assessor (QSA) or Non-PCI Data Security Audit Contractor approved under the CTR Data Security Audits Statewide Contract.

    a. **Application of independent "initial" validation**. This requirement applies to any Department in any Branch of state government accepting payments through collection options ***OTHER than credit and debit cards,*** even though no specific industry standards have been published by NACHA or the Federal Reserve Bank for these types of payment options. Departments accepting electronic payments (other than credit and debit cards) face the same state and federal requirements to prevent data breaches and maintain the security of PII and confidential data. The purpose of this independent validation is to provide documentation of data security due diligence and to document a data security compliance baseline for ongoing compliance and budgeting purposes. Independent "initial" validations of compliance conducted between 2010-2013 by an authorized Qualified Security Assessor (QSA) or other qualified security assessor may be acceptable if the payment environment, software and payment applications for the Department merchant have not materially changed.

    b. **Scope of independent "initial" validation**. An independent data security compliance validation of commercially reasonable data security standards compliance must be made by a Qualified Security Assessor (QSA) or Non-PCI Data Security Audit Contractor approved under the CTR Data Security Audits Statewide Contract for all payment collection methods including but not limited to

payment applications, devices or channels, including but not limited to mail, cashier window, point of sale, telephone, web application, Interactive Voice Response (IVR) or mechanism, and mobile device payments. New e-commerce implementations under the Comptroller E-Pay Statewide Contract are validated during the project development process. Payment collection methods must also be validated for state finance law compliance purposes by the Office of the Comptroller prior to implementation.

c. **Use of Internal Security Assessors (ISA)**. Department merchants whose employees have been trained, tested, qualified and attested with as authorized Payment Card Industry Council Internal Security Assessors (ISA) may **not** conduct the "initial" validation of commercially reasonable data security standards compliance. This Policy requires the initial validation to be conducted by an "independent" Qualified Security Assessor (QSA) or Non-PCI Data Security Audit Contractor approved on the CTR Data Security Audits Statewide Contract. Once the initial validation is completed, the Internal Security Assessor employees of the Department may conduct ongoing security audits.

Statewide Contract for Data Security Audits

The CTR Data Security Audits Statewide Contract has been established by the Office of the Comptroller to support data security compliance and must be used by all Departments (in any branch of government) to meet Payment Card Industry Council and other data security compliance requirements. The Statewide Contract has pre-qualified contractors approved by the Payment Card Industry Council to provide Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV) services as well as other data management security professionals. As this Statewide Contract is procured under the authority of the Comptroller to implement state finance law and prescribe fiscal accountability, Department merchants must use this Statewide Contract to procure the services of QSA professionals and ASVs for Payment Card Industry Council Data Security Standards and for other information management security compliance audits (in any branch of government). These services may not be independently procured under separate general procurement authority.

On-going Data Security Maintenance Obligations

Given the serious consequences of a Commonwealth security compromise and the significant cost to taxpayers for associated notifications, fines, penalties and consumer identify theft damages, the security of personal information such as cardholder, banking data and PII that may be stored, processed or transmitted for Department fiscal business is

essential. Departments must identify resources and funding to support ongoing data security compliance, including:

1) **Training.** Staff should be trained not less regularly than annually on data security responsibilities, and new staff must be trained before being provided access to any PII or before processing payment collections.
2) **Internal Controls.** Rigorous internal controls must be developed and enforced to ensure the protection of any PII and customer or cardholder data that is collected, stored, or transmitted related to fiscal transactions, including payment collections, to prevent unauthorized access, theft, misuse or other actions that might result in a data breach or identify theft.
3) **Initial and on-going data security compliance audits.** As data breaches present a significant financial risk, initial baseline and ongoing data security compliance audits as required in this Policy are a normal operational responsibility and must be budgeted if the Department accepts PII as part of operations, transactions or the collection of payments.

    a) Re-Evaluations if Material Changes. Any Department merchant must engage in independent data security compliance re-evaluations whenever the payment environment changes materially, including but not limited to business applications and systems, hardware and devices, software or other protocols. Payment applications must be re-validated every time the applications, devices (such as mobile devices) are changed or the payment environment materially changes to ensure sufficient data security of cardholder data and PII.

    b) **Annual budget requests.** Departments must ensure that appropriate budget requests to support initial and ongoing data security compliance audits and remediation are filed through the annual budget process. Notification of these budget requirements with the House and Senate Committees on Ways and Means is recommended.

    c) **Budget Reductions under G.L. c, 29, s. 9C**. In the event that funds appropriated or otherwise made available for ongoing mandated obligations under this Policy are reduced due to a G.L. c. 29, s. 9C reduction, a Department is obligated to continue to make budget requests through the normal budget or supplemental budget process, or take other appropriate actions, to restore funds to support data security compliance. Notification to the House and Senate Committees on Ways and Means of the budget reductions and increased security risks is recommended.

d) **Halting use of Credit and Debit Cards for Payment Collections.** In the event a Department is unable to maintain sufficient funds to ensure Payment Card Industry Council Data Security Standards compliance, the Department must halt the continued use of credit and debit cards for payments collection until PCI-DSS compliance can be adequately maintained.

Annual ICQ Data Security Certification. Departments are now required to certify compliance with this Policy under the Office of the Comptroller annual Internal Control Questionnaire (ICQ) process. In the event that a Department merchant is not required to file the annual ICQ or does not file the ICQ, the Department merchant is required to maintain documentation of compliance for state finance law purposes to ensure fiscal responsibility of taxpayer funds (to avoid the costs of a data breach) and to protect taxpayers and other customers from the costs of a data breach.

Data Breach Prevention and Notice Responsibilities.

Departments are responsible for compliance with data breach prevention prescribed by the Office of the Attorney General (see http://www.mass.gov/ago/doing-business-in-massachusetts/privacy-and-data-security/security-breaches.html) and under Executive Order 504 (Executive Departments) and any other published guidance for the Department's activities.

Commonwealth Departments are required to comply with all applicable state and federal privacy laws, regulations and policies including but not limited to 940 CMR 27.00 (http://www.mass.gov/ago/docs/regulations/940-cmr-27-00.pdf), G.L. c. 93H and c. 93I; Executive Order 504 (Executive Departments), disclosure exemptions under G.L. c. 66 (http://www.malegislature.gov/Laws/GeneralLaws/PartI/TitleX/Chapter66); and the Fair Information Practices Act under G.L. c. 66. (http://www.malegislature.gov/Laws/GeneralLaws/PartI/TitleX/Chapter66A).

Departments subject to a data breach are required to follow the procedures for notifying the Information Technology Division and the Office of the Attorney General prescribed by G.L. c. 93H (c), and the procedures for notifying the consumer prescribed by the G.L. c. 93H and by the Attorney General and the Office of Consumer Affairs and Business Regulation, and must notify the Office of the Comptroller and the Executive Office for Administration and Finance of any budget deficiency and accounting issues related to compliance with data breach notifications and costs. Department data owners responsible for actions or inactions

that result in a data breach will be responsible for providing all notices to customers or affected parties and the costs of all damages, penalties, compliance or remediation costs assessed by the card associations or through consumer lawsuits and remediation necessary to rectify the data security weakness and internal controls.

In the event the Department responsible for the data breach hosts (even through a third party) the system, application or process that collected, stored, processed, or transmitted the data subject to the data breach, that Department (even though not a holder of the data) shall be responsible for cooperating with the data holder of the data to meet the notice requirements for the data breach and may be responsible for seeking funding for the costs of the data breach and taking appropriate steps to remediate the hosted system, application or process to rectify the data security weakness and internal controls.

Records Management

A Department is the keeper of the official record copy of all documents and records supporting fiscal transactions including the acceptance of payments. The state accounting system MMARS will be the official record copy of the transaction or payments receipt documents recording payments that will supersede any paper copies of the same transactions or documents. A Department is responsible for retaining and archiving all records related to data security compliance and payments receipt records in accordance with the disposal schedules issued by the Secretary of State Records Conservation Board.

Violation of State Finance Law

Any Department head or designee who knowingly violates state finance law, authorizes or directs another officer or employee to violate any provision of G.L. c. 29, or any rule or regulation promulgated there under, or any other provision of law relating to the incurring of liability or expenditure of public funds, shall be punishable by fine of $1,000 or imprisonment for one year, or both. See G.L. c.29, § 66 .

Internal Controls

A Department is responsible for updating its internal controls as documented in its Internal Control Plan to support the requirements under this Policy. See guidance under Internal Controls http://www.mass.gov/osc/guidance-for-agencies/internal-controls.html and Internal Controls for Revenue Appendix at http://www.mass.gov/osc/docs/business-functions/bf-int-cntrls/osc-icg-01-appendices.pdf.

Quality Assurance

The Office of the Comptroller will interpret this policy and take any actions necessary to carry out the security purposes of this policy, including issuing additional policies, procedures and forms for Department use. The Office of the Comptroller may review any payments collection activities of a Department to ensure compliance under this policy and may recommend any actions necessary to achieve or maintain compliance.

Information Sources

- G.L. c. 7A (Office of the Comptroller);
- G.L. c. 29 (State Finance Law);
- G.L. c.29, § 66 (State Finance Law Violations)
- G.L. c. 66A Fair Information Practices Act
- 801 CMR 3 Privacy and Confidentiality
- G.L. c.214 s. 1B Right to Privacy
- GL c.214 s. 3B Violations of Chapter 66A; Statute of Limitations
- Security Breaches G.L. c. 93H

Related Policies:

- Key State Finance Law Compliance Appointments and Responsibilities
- Department Head Signature Authorization and Electronic Signature for MMARS Documents
- EOTSS Security Policies
- Non-Tax Revenue Policies
- Contacts – CTR Help Desk 617-973-2468
- Comptroller Website

Revisions