
# Payment Card Industry (PCI)
# Data Security Standard

---

# Attestation of Compliance for Onsite Assessments – Service Providers

**Version 3.2.1**

Revision 2

September 2022

# Document Changes

| Date | Version | Description |
|---|---|---|
| September 2022 | 3.2.1 Revision 2 | Updated to reflect the inclusion of UnionPay as a Participating Payment Brand. |

# Section 1: Assessment Information

### *Instructions for Submission*

This Attestation of Compliance must be completed as a declaration of the results of the service provider's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS).* Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

| **Part 1. Service Provider and Qualified Security Assessor Information** | | | | | |
|---|---|---|---|---|---|
| **Part 1a. Service Provider Organization Information** | | | | | |
| Company Name: | AvidXchange Inc. | | DBA (doing business as): | N/A | |
| Contact Name: | Christina Quaine | | Title: | Chief Information Security Officer, SVP Technology Operations | |
| Telephone: | 313-319-7837 | | E-mail: | cquaine@avidxchange.com | |
| Business Address: | 1210 AvidXchange Lane | | City: | Charlotte | |
| State/Province: | NC | Country: | USA | Zip: | 28206 |
| URL: | avidxchange.com | | | | |

| **Part 1b. Qualified Security Assessor Company Information (if applicable)** | | | | | |
|---|---|---|---|---|---|
| Company Name: | Agio Inc. | | | | |
| Lead QSA Contact Name: | Virginia Carty | | Title: | Associate Director, Cyber & Compliance | |
| Telephone: | 919-812-0770 | | E-mail: | virginia.carty@agio.com | |
| Business Address: | 292 Madison Avenue Floor 22 | | City: | New York | |
| State/Province: | NY | Country: | USA | Zip: | 10017 |
| URL: | https://agio.com | | | | |

## Part 2. Executive Summary

### Part 2a. Scope Verification

**Services that were INCLUDED in the scope of the PCI DSS Assessment** (check all that apply):

| Name of service(s) assessed: | Accounts payable automation solutions and services | |
|---|---|---|
| Type of service(s) assessed: | | |
| **Hosting Provider:**<br>☐ Applications / software<br>☐ Hardware<br>☐ Infrastructure / Network<br>☐ Physical space (co-location)<br>☐ Storage<br>☐ Web<br>☐ Security services<br>☐ 3-D Secure Hosting Provider<br>☐ Shared Hosting Provider<br>☐ Other Hosting (specify):<br>Not applicable. AvidXchange is not a hosting provider. | **Managed Services (specify):**<br>☐ Systems security services<br>☐ IT support<br>☐ Physical security<br>☐ Terminal Management System<br>☐ Other services (specify):<br>Not applicable. AvidXchange is not a managed service provider. | **Payment Processing:**<br>☐ POS / card present<br>☐ Internet / e-commerce<br>☐ MOTO / Call Center<br>☐ ATM<br>☐ Other processing (specify):<br>Not applicable. AvidXchange does not process credit card transactions. |
| ☐ Account Management | ☐ Fraud and Chargeback | ☐ Payment Gateway/Switch |
| ☐ Back-Office Services | ☒ Issuer Processing | ☐ Prepaid Services |
| ☐ Billing Management | ☐ Loyalty Programs | ☐ Records Management |
| ☐ Clearing and Settlement | ☐ Merchant Services | ☐ Tax/Government Payments |
| ☐ Network Provider | | |
| ☐ Others (specify): N/A | | |

***Note**: These categories are provided for assistance only, and are not intended to limit or predetermine an entity's service description. If you feel these categories don't apply to your service, complete "Others." If you're unsure whether a category could apply to your service, consult with the applicable payment brand.*

## Part 2a. Scope Verification (continued)

**Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment (check all that apply):**

| Name of service(s) not assessed: | Not applicable. All PCI-relevant services were assessed as part of the ROC. |
|---|---|

Type of service(s) not assessed:

| **Hosting Provider:** | **Managed Services (specify):** | **Payment Processing:** |
|---|---|---|
| ☐ Applications / software | ☐ Systems security services | ☐ POS / card present |
| ☐ Hardware | ☐ IT support | ☐ Internet / e-commerce |
| ☐ Infrastructure / Network | ☐ Physical security | ☐ MOTO / Call Center |
| ☐ Physical space (co-location) | ☐ Terminal Management System | ☐ ATM |
| ☐ Storage | ☐ Other services (specify): | ☐ Other processing (specify): |
| ☐ Web | Not applicable. All PCI-relevant services were assessed as part of the ROC. | Not applicable. AvidXchange does not process credit card transactions. |
| ☐ Security services | | |
| ☐ 3-D Secure Hosting Provider | | |
| ☐ Shared Hosting Provider | | |
| ☐ Other Hosting (specify): Not applicable. All PCI-relevant services were assessed as part of the ROC. | | |
| ☐ Account Management | ☐ Fraud and Chargeback | ☐ Payment Gateway/Switch |
| ☐ Back-Office Services | ☐ Issuer Processing | ☐ Prepaid Services |
| ☐ Billing Management | ☐ Loyalty Programs | ☐ Records Management |
| ☐ Clearing and Settlement | ☐ Merchant Services | ☐ Tax/Government Payments |
| ☐ Network Provider | | |
| ☐ Others (specify): Not applicable. All PCI-relevant services were assessed as part of the ROC. | | |

| Provide a brief explanation why any checked services were not included in the assessment: | Not applicable. All PCI-relevant services were assessed as part of the ROC. |
|---|---|

## Part 2b. Description of Payment Card Business

| Describe how and in what capacity your business stores, processes, and/or transmits cardholder data. | Established in Charlotte, NC, in 2000, AvidXchange Inc. (AvidXchange) is a technology company specializing in accounts payable automation solutions. AvidXchange aims to help its clients cut costs, improve visibility, and increase efficiencies across its accounts payable operations. AvidXchange supports more than 8,000 middle-market companies by coordinating bill payments to the over 965,000 suppliers (vendors, service providers, etc.) within the AvidPay network, amounting to over 70,000,000 transactions annually.<br>AvidXchange uses one-time-use credit cards, issued by Mastercard, to make payments to suppliers on behalf of AvidXchange's clients. Cards are usually issued for specific amounts for each individual transaction, and expiry dates are set close |
|---|---|

| | |
|---|---|
| | to the date of issuance. Payments are typically processed as soon as the card number is provided to AvidXchange. Cards are issued in the name of the business (AvidXchange's client), and because AvidXchange's processes do not support recurring payments, card numbers are different every time and are never reused.<br>AvidXchange makes payments via a variety of payment methods:<br>• Twilio and NICE services and software are leveraged to make automated payments to suppliers' IVR systems and traditional phone calls directly to the supplier/payee. Call recordings are captured and retained by both Twilio and NICE.<br>• Fax CHD payments leverage OpenText, a web-based e-fax client.<br>• Payments made via web portals are submitted through applications, and systems are entirely operated and maintained by individual suppliers.<br>• Some payments are made via SFTP. In this use case, AvidXchange uploads text or Excel files containing CHD to servers maintained by suppliers.<br>• Some suppliers request that card numbers be emailed to them. In those cases, AvidXchange will provide a link via email that allows the supplier to retrieve a token. (AvidXchange leverages TokenEx for tokenization services.) When the supplier clicks the emailed link, the response back to the supplier is delivered straight to the client's browser via an inline frame.<br>• Suppliers have the ability, through the portal, to click and view the full card number.<br>• Some payments are triggered automatically via business logic and submitted to NMI for processing of payments. |
| Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data. | AvidXchange uses one-time-use credit cards, issued by Mastercard, to make payments to suppliers on behalf of AvidXchange's clients. Cards are usually issued for specific amounts for each individual transaction, and expiry dates are set close to the date of issuance. Payments are typically processed as soon as the card number is provided to AvidXchange. Cards are issued in the name of the business (AvidXchange's client), and because AvidXchange's processes do not support recurring payments, card numbers are different every time and are never reused.<br>AvidXchange makes payments via a variety of payment methods:<br>• Twilio and NICE services and software are leveraged to make automated payments to suppliers' IVR systems and traditional phone calls directly to the supplier/payee. Call recordings are captured and retained by both Twilio and NICE.<br>• Fax CHD payments leverage OpenText, a web-based e-fax client.<br>• Payments made via web portals are submitted through applications, and systems are entirely operated and maintained by individual suppliers.<br>• Some payments are made via SFTP. In this use case, AvidXchange uploads text or Excel files containing CHD to servers maintained by suppliers.<br>• Some suppliers request that card numbers be emailed to them. In those cases, AvidXchange will provide a link via email that allows the supplier to retrieve a token. (AvidXchange leverages TokenEx for tokenization services.) When the supplier clicks the emailed link, the response back to the supplier is delivered straight to the client's browser via an inline frame.<br>• Suppliers have the ability, through the portal, to click and view the full card number.<br>• Some payments are triggered automatically via business logic and submitted to NMI for processing of payments. |

## Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

| Type of facility: | Number of facilities of this type | Location(s) of facility (city, country): |
|---|---|---|
| *Example: Retail outlets* | *3* | *Boston, MA, USA* |
| Azure environment | 1 | East US (Virginia, USA) |
| AvidXchange offices | 2 | Sandy, UT, and Charlotte, NC |
| | | |

## Part 2d. Payment Applications

Does the organization use one or more Payment Applications? ☐ Yes ☒ No

Provide the following information regarding the Payment Applications your organization uses:

| Payment Application Name | Version Number | Application Vendor | Is application PA-DSS Listed? | PA-DSS Listing Expiry date (if applicable) |
|---|---|---|---|---|
| N/A | N/A | N/A | N/A | N/A |
| | | | | |

## Part 2e. Description of Environment

Provide a ***high-level*** description of the environment covered by this assessment.

*For example:*
- *Connections into and out of the cardholder data environment (CDE).*
- *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*

The following payment channels were validated as part of this assessment:

- Twilio and NICE services and software are leveraged to make automated payments to suppliers' IVR systems, and traditional phone calls are made directly to the supplier/payee. Call recordings are captured and retained by both Twilio and NICE.
- Fax CHD payments leverage OpenText, a web-based e-fax client.
- Payments made via web portals are submitted through applications, and systems are entirely operated and maintained by individual suppliers.
- Some payments are made via SFTP. In this use case, AvidXchange uploads text or Excel files containing CHD to servers maintained by suppliers.
- Some suppliers request that card numbers be emailed to them. In those cases, AvidXchange will provide a link via email that allows the supplier to retrieve a token. (AvidXchange leverages TokenEx for tokenization services.) When the supplier clicks the emailed link, the response back to the supplier is delivered straight to the client's browser via an inline frame.
- Suppliers have the ability, through the portal, to click and view the full card number.
- Some payments are triggered automatically via business logic and submitted to NMI for processing of payments.

The following direct connections to outside entities were reviewed as part of this assessment:

- NICE - Call center software used to make CHD payments and record phone calls
- TokenEx - Tokenization services for CHD

| | |
|---|---|
| | • NMI, Comdata, and WEX - Virtual credit card processing<br>• Twilio - Solution integrated with automated IVR process used to submit CHD payments and record phone calls<br>The following critical technologies were deemed in-scope for this assessment:<br>• Azure-hosted PCI environment<br>• Azure subscription-based segmentation<br>• Workstations (Windows 10)<br>• Firewall + IDS/IPS (Check Point)<br>• Meraki WAPs and Air Marshal<br>• Arctic Wolf (SIEM)<br>• Servers (Windows Server 2016)<br>• Load balancers, WAF, application gateway (Microsoft Azure)<br>• VPN (Cisco AnyConnect)<br>• Portnox<br>• Two-factor authentication (Microsoft Authenticator)<br>• AvidPay (B2B hub for payment operations)<br>• TLS and SFTP<br>• Remote Desktop Protocol<br>• Active Directory |
| Does your business use network segmentation to affect the scope of your PCI DSS environment?<br>*(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)* | ☒ Yes ☐ No |

| Part 2f. Third-Party Service Providers | |
|---|---|
| Does your company have a relationship with a Qualified Integrator & Reseller (QIR) for the purpose of the services being validated? | ☐ Yes ☒ No |
| ***If Yes:*** | |
| Name of QIR Company: | N/A |
| QIR Individual Name: | N/A |
| Description of services provided by QIR: | N/A |
| Does your company have a relationship with one or more third-party service providers (for example, Qualified Integrator Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated? | ☒ Yes ☐ No |
| ***If Yes:*** | |

| **Name of service provider:** | **Description of services provided:** |
|---|---|
| Microsoft (Azure) | Cloud hosting for CDE |
| NICE Ltd. | Call center software used to make CHD payments and record phone calls |
| TokenEx | Tokenization services for CHD |
| WEX | Virtual credit card processing |
| OpenText | Fax solution used to send CHD payments |
| Comdata | Virtual credit card processing |
| NMI | Virtual credit card processing |
| Twilio | Solution integrated with automated IVR process used to submit CHD payments and record phone calls |
| Excela | Virtual card processing |

***Note:*** *Requirement 12.8 applies to all entities in this list.*

## Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- **Full** – The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as "Not Tested" or "Not Applicable" in the ROC.
- **Partial** – One or more sub-requirements of that requirement were marked as "Not Tested" or "Not Applicable" in the ROC.
- **None** – All sub-requirements of that requirement were marked as "Not Tested" and/or "Not Applicable" in the ROC.

For all requirements identified as either "Partial" or "None," provide details in the "Justification for Approach" column, including:

- Details of specific sub-requirements that were marked as either "Not Tested" and/or "Not Applicable" in the ROC
- Reason why sub-requirement(s) were not tested or not applicable

***Note:*** *One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.*

| **Name of Service Assessed:** | Accounts payable automation solutions and services; issuer processing |
|---|---|

| PCI DSS Requirement | Details of Requirements Assessed | | | |
|---|---|---|---|---|
| | **Full** | **Partial** | **None** | **Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.) |
| Requirement 1: | ☐ | ☒ | ☐ | 1.1.6.b, 1.1.6.c - No insecure services, protocols, or ports are allowed.<br>1.3.6 - No system components store cardholder data. |
| Requirement 2: | ☐ | ☒ | ☐ | 2.2.2.b, 2.2.3 - No insecure services, daemons, or protocols are allowed.<br>2.6 - AvidXchange is not a shared hosting provider. |
| Requirement 3: | ☐ | ☒ | ☐ | 3.1.b–3.1.c, 3.2, 3.4, 3.5, 3.6 - AvidXchange does not store CHD.<br>3.2.1, 3.2.3 - AvidXchange is never in possession of full track data, PINs, or PIN blocks.<br>3.3 - No employees have access to visual displays of PAN (paper or electronic). |
| Requirement 4: | ☐ | ☒ | ☐ | 4.2.a - End-user messaging technologies are not used to transmit CHD. |
| Requirement 5: | ☐ | ☒ | ☐ | 5.1.2 - All in-scope systems capable of running AV have an AV solution installed. |

| PCI DSS Requirement | Details of Requirements Assessed | | | |
|---|---|---|---|---|
| | Full | Partial | None | Justification for Approach<br>(Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.) |
| Requirement 6: | ☐ | ☒ | ☐ | 6.3.2.b, 6.4.5.3.b - AvidXchange did not make any PCI-applicable code changes that would affect the security of CHD during the assessment period.<br>6.4.4 - Accounts for development/test/QA are separate from those used for production and only exist in a separate development environment.<br>6.4.6 - No significant changes were made in the period of time covered by this assessment. |
| Requirement 7: | ☒ | ☐ | ☐ | |
| Requirement 8: | ☐ | ☒ | ☐ | 8.1.5 - No third parties have access to AvidXchange's PCI environment.<br>8.1.6.b, 8.2.1.d, 8.2.1.e, 8.2.3.b, 8.2.4.b, 8.2.5.b - AvidXchange does not create or support nonconsumer customer/user accounts.<br>8.5.1 - AvidXchange is not a shared hosting provider and does not have access to customer accounts or environments.<br>8.7 - AvidXchange does not maintain databases containing CHD. |
| Requirement 9: | ☐ | ☒ | ☐ | 9.1.2 - No publicly accessible locations are in scope.<br>9.5–9.8 - AvidXchange does not maintain media containing CHD.<br>9.9 - AvidXchange does not capture CHD via swipe devices. |
| Requirement 10: | ☐ | ☒ | ☐ | 10.2.1 - No AvidXchange employees have access to full CHD.<br>10.8.1.b - AvidXchange did not experience an in-scope security control failure in the previous year. |
| Requirement 11: | ☐ | ☒ | ☐ | 11.1.d - Wireless IDS/IPS or NAC is not used to detect rogue WAPs.<br>11.2.1 - This requirement was not tested during the assessment.<br>11.2.3 - No significant changes have been made in the period of time covered by this assessment.<br>11.3.1.b, 11.3.2.b - The penetration test was performed by a third party. |
| Requirement 12: | ☒ | ☐ | ☐ | |
| Appendix A1: | ☐ | ☐ | ☒ | AvidXchange is not a shared hosting provider. |
| Appendix A2: | ☐ | ☐ | ☒ | AvidXchange does not leverage POS POI terminals using SSL/early TLS. |

## Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

| | |
|---|---|
| The assessment documented in this attestation and in the ROC was completed on: | June 30, 2023 |
| Have compensating controls been used to meet any requirement in the ROC? | ☐ Yes ☒ No |
| Were any requirements in the ROC identified as being not applicable (N/A)? | ☒ Yes ☐ No |
| Were any requirements not tested? | ☒ Yes ☐ No |
| Were any requirements in the ROC unable to be met due to a legal constraint? | ☐ Yes ☒ No |

# Section 3: Validation and Attestation Details

## Part 3. PCI DSS Validation

**This AOC is based on results noted in the ROC dated June 30, 2023.**

Based on the results documented in the ROC noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document (***check one):***

| | |
|---|---|
| ☒ | **Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby AvidXchange Inc. has demonstrated full compliance with the PCI DSS. |
| ☐ | **Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby AvidXchange Inc. has not demonstrated full compliance with the PCI DSS.<br>**Target Date** for Compliance: N/A<br>An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with the payment brand(s) before completing Part 4.* |
| ☐ | **Compliant but with Legal exception:** One or more requirements are marked "Not in Place" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand.<br>*If checked, complete the following:* |

| Affected Requirement | Details of how legal constraint prevents requirement being met |
|---|---|
| | |
| | |

## Part 3a. Acknowledgement of Status

**Signatory(s) confirms:**

***(Check all that apply)***

| | |
|---|---|
| ☒ | The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version 3.2.1 Revision 2, and was completed according to the instructions therein. |
| ☒ | All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects. |
| ☐ | I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization. |
| ☒ | I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times. |
| ☒ | If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply. |

| Part 3a. Acknowledgement of Status (continued) | |
|---|---|
| ☒ | No evidence of full track data[1], CAV2, CVC2, CVN2, CVV2, or CID data[2], or PIN data [3] storage after transaction authorization was found on ANY system reviewed during this assessment. |
| ☒ | ASV scans are being completed by the PCI SSC Approved Scanning Vendor Qualys Inc. |

**Part 3b. Service Provider Attestation**

Christina Quaine

| | | | |
|---|---|---|---|
| *Signature of Service Provider Executive Officer ↑* | | *Date:* | June 30, 2023 |
| *Service Provider Executive Officer Name:* | Christina Quaine | *Title:* | Chief Information Security Officer, SVP Technology Operations |

**Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)**

| | |
|---|---|
| If a QSA was involved or assisted with this assessment, describe the role performed: | The QSA validated evidence submitted by the service provider and performed interviews and observations to satisfy all applicable PCI DSS requirement testing procedures. |

Bart R. McDonough

| | | | |
|---|---|---|---|
| *Signature of Duly Authorized Officer of QSA Company ↑* | | *Date:* | June 30, 2023 |
| *Duly Authorized Officer Name:* | Bart R. McDonough | *QSA Company:* | Agio Inc |

**Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)**

| | |
|---|---|
| If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed: | Not applicable |

[1] Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

[2] The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

[3] Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

## Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement. If you answer "No" to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

*Check with the applicable payment brand(s) before completing Part 4.*

| PCI DSS Requirement | Description of Requirement | Compliant to PCI DSS Requirements *(Select One)* | | Remediation Date and Actions (If "NO" selected for any Requirement) |
|---|---|---|---|---|
| | | YES | NO | |
| 1 | Install and maintain a firewall configuration to protect cardholder data | ☒ | ☐ | N/A |
| 2 | Do not use vendor-supplied defaults for system passwords and other security parameters | ☒ | ☐ | N/A |
| 3 | Protect stored cardholder data | ☒ | ☐ | N/A |
| 4 | Encrypt transmission of cardholder data across open, public networks | ☒ | ☐ | N/A |
| 5 | Protect all systems against malware and regularly update anti-virus software or programs | ☒ | ☐ | N/A |
| 6 | Develop and maintain secure systems and applications | ☒ | ☐ | N/A |
| 7 | Restrict access to cardholder data by business need to know | ☒ | ☐ | N/A |
| 8 | Identify and authenticate access to system components | ☒ | ☐ | N/A |
| 9 | Restrict physical access to cardholder data | ☒ | ☐ | N/A |
| 10 | Track and monitor all access to network resources and cardholder data | ☒ | ☐ | N/A |
| 11 | Regularly test security systems and processes | ☒ | ☐ | N/A |
| 12 | Maintain a policy that addresses information security for all personnel | ☒ | ☐ | N/A |
| Appendix A1 | Additional PCI DSS Requirements for Shared Hosting Providers | ☒ | ☐ | N/A |
| Appendix A2 | Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections | ☒ | ☐ | N/A |