# DISTRICT SCHOOL BOARD OF PASCO COUNTY

Kurt S. Browning, Superintendent of Schools

7227 Land O' Lakes Boulevard • Land O' Lakes, Florida 34638

Purchasing Services
Nicole Westmoreland, MBA, Purchasing Agent
813/ 794-2221 Fax: 813/ 794-2111
727/ 774-2221 TDD: 813/794-2484
352/ 524-2221 e-mail: nwestmor@pasco.k12.fl.us


May 20, 2014

MEMORANDUM

TO: Honorable School Board Members

FROM: Nicole Westmoreland, MBA, Purchasing Agent NW

SUBJECT: My Payment Network Merchant Services Agreement

Attached is an agreement between My Payment Network dba SchoolPay and the District School Board of Pasco County that will provide Pasco County parents the opportunity to make online payments with their credit or debit card for many school expenses. My Payment Network, Inc. is the leading eCommerce provider to K12, delivering services to schools and the vendors that serve schools, through its MyPayNet (http://www.mypaynet.com) and SchoolPay (www.schoolpay.com ). My Payment Network is Payment Card Industry Data Security Standard (PCI) compliant and as such requires the District to adhere to the PCI standards. Parent and other users data is protected under these guidelines.

**SchoolPay offers several benefits to our Pasco families:**

- Pay online via VISA, MasterCard, Discover cards and electronic check
- Make payments from a secure parent account with just a few clicks
- A full history of payments searchable by date and child
- The convenience of paying at any time (24/7) from home
- Schools will be able to accept credit/debit cards on site

This agreement shall remain in effect for a period of two (2) years with annual renewal, upon Board approval. Content of the agreement was reviewed and approved by Nancy Alfonso, School Board attorney, on April 24, 2014.

The District School Board of Pasco County will pay a one-time set up fee of $2,000 and an annual fee of $1,400. Transaction fees will be based on the rates approved by the Orange County Public Schools RFP #1101024: Cost plus .49% + $.10 per transaction for Visa, MasterCard, and Discover credit card transactions. There will be a convenience fee charged to the parent for usage of the program that will help defer the costs incurred by the District.

SchoolPay will provide training for all bookkeepers in July; each bookkeeper will need one 2+ hour session with a computer. SchoolPay will also schedule Webinars during the weeks of June 9-13 and June 16-20 for bookkeepers to practice using their own computers at their school. This will ensure that the trainings in July will be the most effective.

Should you have any questions regarding this matter, please contact Ray Bonti, Executive Director for Support Services, or Debra Reaves, Purchasing Services, at your earliest convenience.

NW/dr
Attachments

Date/Time: May 14, 2014 09:46:00

MyPayment NETWORK

# *MERCHANT SERVICES AGREEMENT for SUB-MERCHANTS*

In connection with Pasco County Public Schools ("Merchant") with tax ID_____and in agreement with My Payment Network, Inc. ("Provider"), Vantiv, LLC and its designated Member Bank (collectively "Vantiv") will provide Merchant with certain payment processing services ("Services") in accordance with the terms of this Merchant Services Agreement. In consideration of Merchant's receipt of credit or debit card funded payments, and participation in programs affiliated with MasterCard International Inc. ("MasterCard"), VISA U.S.A. Inc. ("VISA"), Discover ("Discover"), and certain similar entities (collectively, "Associations), Merchant is required to (i) enter into a direct relationship with an entity that is a member of the Associations and (ii) agree to comply with Association rules as they pertain to applicable credit and debit card payments. By executing this Merchant Services Agreement, Merchant is fulfilling the Association rule of entering into a direct relationship with a Member of the Associations; however, Vantiv understands that Merchant may have contracted with Provider to obtain certain processing services and that Provider may have agreed to be responsible to Merchant for all or part of Merchant's obligations contained herein.

NOW, THEREFORE, in consideration of the foregoing recitals and of the mutual promises contained herein, the parties agree as follows:

1. **Certain Merchant Responsibilities.**

Merchant agrees to participate, and to cause third parties acting as Merchant's agent ("Agents"), to participate, in the Associations in compliance with, and subject to, the by-laws, operating regulations and/or all other rules, policies and procedures of the Associations (collectively "Operating Regulations"). Merchant also agrees to comply with all applicable state, federal, and local laws, rules, and regulations ("Laws"). Without limiting the foregoing, Merchant agrees that it will fully comply with any and all confidentiality and security requirements of the USA Patriot Act (or similar law, rule or regulation), VISA, MasterCard, Discover, and/or Other Networks, including but not limited to the Payment Card Industry Data Security Standard, the VISA Cardholder Information Security Program, the MasterCard Site Data Protection Program, and any other program or requirement that may be published and/or mandated by the Associations. For purposes of this section, Agents include, but are not limited to, Merchant's software providers and/or equipment providers.

If appropriately indicated in Merchant's agreement with Provider, Merchant may be a limited-acceptance Merchant, which means that Merchant has elected to accept only certain Visa and MasterCard card types (i.e., consumer credit, consumer debit, and commercial cards) and must display appropriate signage to indicate the same. Vantiv has no obligation other than those expressly provided under the Operating Regulations and applicable law as they may relate to limited acceptance. Merchant, and not Vantiv, will be solely responsible for the implementation of its decision for limited acceptance, including but not limited to policing the card type(s) accepted at the point of sale.

Merchant shall only complete sales transactions produced as the direct result of bona fide sales made by Merchant to cardholders, and is expressly prohibited from processing, factoring, laundering, offering, and/or presenting sales transactions which are produced as a result of sales made by any person or entity other than Merchant, or for purposes related to financing terrorist activities.

Merchant may set a minimum transaction amount to accept a card that provides access to a credit account, under the following conditions: i) the minimum transaction amount does not differentiate between card issuers; ii) the minimum transaction amount does not differentiate between MasterCard, Visa, or any other acceptance brand; and iii) the minimum transaction amount does not exceed ten dollars (or any higher amount established by the Federal Reserve). Merchant may set a maximum transaction amount to accept a card that provides access to a credit account, under the following conditions: Merchant is a i) department, agency or instrumentality of the U.S. government; ii) corporation owned or controlled by the U.S. government; or iii) Merchant whose primary business is reflected by one of the following MCCs: 8220, 8244, 8249 –Schools, Trade or Vocational; and the maximum transaction amount does not differentiate between MasterCard, Visa, or any other acceptance brand.

2. **Merchant Prohibitions.**

Merchant must not i) require a cardholder to complete a postcard or similar device that includes the cardholder's account number, card expiration date, signature, or any other card account data in plain view when mailed, ii) add any tax to transactions, unless applicable law expressly requires that a Merchant impose a tax (any tax amount, if allowed, must be included in the transaction amount and not collected separately), iii) request or use an account number for any purpose other than as payment for its goods or services, iv) disburse funds in the form of travelers checks if the sole purpose is to allow the cardholder to make a cash purchase of goods or services from Merchant, v) disburse funds in the form of cash unless Merchant is dispensing funds in the form of travelers checks, TravelMoney cards, or foreign currency (in such case, the transaction amount is limited to the value of the travelers checks, TravelMoney cards, or foreign currency, plus any commission or fee charged by the Merchant), or Merchant is participating in a cash back service, vi) submit any transaction receipt for a transaction that was previously charged back to the acquirer and subsequently returned to Merchant, irrespective of cardholder approval, vii) accept a Visa consumer credit card or commercial Visa product issued by a U.S. issuer to collect or refinance an existing debt, viii) accept a card to collect or refinance an existing debit that has been deemed uncollectable by Merchant, or ix) submit a transaction that represents collection of a dishonored check. Merchant further agrees that, under no circumstance, will Merchant store cardholder data in violation of the Laws or the Operating Regulations including but not limited to the storage of track-2 data. Neither Merchant nor its Agent shall retain or store magnetic-stripe data subsequent to the authorization of a sales transaction.



CONTRACT REVIEWED AND APPROVED:
NW 5-12-14

MyPayment NETWORK

3. **Settlement.**

Upon receipt of Merchant's sales data for card transactions through Provider Services, Vantiv will process Merchant's sales data to facilitate the funds transfer between the various Associations and Merchant. After Vantiv receives credit for such sales data, Vantiv will fund Merchant, either directly to the Merchant-Owned Designated Account or through Provider to an account designated by Provider ("Provider Designated Account"), at Vantiv's sole option, for such card transactions. Merchant agrees that the deposit of funds to the Provider Designated Account shall discharge Vantiv of its settlement obligation to Merchant, and that any dispute regarding the receipt or amount of settlement shall be between Provider and Merchant. Vantiv will debit the Provider Designated Account for funds owed to Vantiv as a result of the Services provided hereunder, unless a

Merchant-owned account is otherwise designated below. Further, if a cardholder disputes a transaction, if a transaction is charged back for any reason, or if Vantiv reasonably believes a transaction is unauthorized or otherwise unacceptable, the amount of such transaction may be charged back and debited from Merchant or Provider.

Merchant-Owned Designated Account
Name of Bank: _____
ABA No.: _____
Account No. _____
Account Name: _____

4. **Term and Termination**

This Merchant Services Agreement shall be binding upon Merchant upon Merchant's execution and remain effect for a period of two (2) years.

Notwithstanding the foregoing, Vantiv may immediately cease providing Services and/or terminate this Merchant Services Agreement without notice if (i) Merchant or Provider fails to pay any amount to Vantiv when due, (ii) in Vantiv's opinion, provision of a service to Merchant or Provider may be a violation of the Operating Regulations, or any applicable state, federal, or local laws, rules, and regulations ("Laws"), (iii) Vantiv believes that Merchant has violated or is likely to violate the Operating Regulations or the Laws, or iv) Vantiv is required to do so by any of the Associations.

5. **Indemnification and Limits of Liability.**

Merchant agrees to provide Vantiv with written notice, specifically detailing any alleged failure, within thirty (30) days of the date on which the alleged failure or error first occurred; failure to so provide notice shall be deemed an acceptance by Merchant and a waiver of any and all rights to dispute such failure or error. Vantiv shall bear no liability and have no obligations to correct any errors resulting from Merchant's failure to comply with the duties and obligations of the preceding sentence

Merchant shall indemnify and hold harmless Vantiv, and its directors, officers, employees, affiliates, and agents from and against all proceedings, claims, demands, losses, liabilities, damages and expenses resulting from or otherwise arising out of (i) the Services in this Merchant Services Agreement, (ii) Merchant's or Merchant's employees and agents acts or omissions in connection with the Services provided pursuant to this Merchant Services Agreement, (iii) any infiltration, hack, breach, or violation of the processing system resulting from, arising out of, or in any way related to Merchant's ability to use of the services provided herein including but not limited to Merchant's use of an Agent or any other third party processor or system or (iv) any issue between Merchant and Provider. This indemnification shall survive the termination of the Agreement. Vantiv's liability related to or arising out of this Merchant Services Agreement shall in no event exceed $5,000. Merchant's sole and exclusive remedy for any and all claims against Vantiv arising out of or in any way related to the transactions contemplated herein shall be termination of this Merchant Services Agreement. Merchant acknowledges that Vantiv is not liable for any action or failure to act by Provider, and that Merchant shall have no liability whatsoever in connection with any products or services provided to Merchant by Provider.

6. **Exception Items; Risk Monitoring Programs.**

Merchant agrees to reacquire and pay Vantiv the amount of any sales transaction, and Vantiv shall have the right at any time to charge Merchant's Account therefore with notice in accordance with Vantiv's standard operating procedure, for any return (whether or not a credit voucher is delivered to Vantiv), chargeback, compliance case, any other Association action, or if the extension of credit for merchandise sold or services or sales transactions performed was in violation of law or the rules or regulations of any governmental agency, federal, state, local or otherwise; or if Vantiv has not received payment for any sales transaction, notwithstanding Vantiv's prior payment to Merchant for such sales transaction pursuant to Section 3 above or any other section. Not limiting the generality of the foregoing, Merchant agrees that any operational and/or other Services performed on behalf of Merchant, including but not limited to, production of facsimile drafts in response to copy requests, response to compliance cases, augmentation of Merchant data for interchange, transaction stand-in, digital draft storage and retrieval, etc. shall in no way affect Merchant's obligations and liability in



CONTRACT REVIEWED AND APPROVED:
NW 5-12-14

this Agreement including those in the foregoing sentence. Merchant may instruct Vantiv in the defense of chargebacks, compliance cases and similar actions, and Merchant agrees that it will promptly provide any such instructions to Vantiv. In order to monitor potential economic hardship or damage to the goodwill of the Associations, the Associations haveimplemented merchant review programs to identify questionable business activity or merchants whose sales transactions generate excessive Cardholder complaints, chargebacks or other disputes. These review programs include potential fines and handling fees. In the event any fees, fines or penalties resulting from Merchant's sales transactions are levied against Vantiv for any reason, Merchant shall reimburse Vantiv on demand or Vantiv may, at its sole option, charge Merchant's Account. In the event Merchant or any of its locations are identified by such review programs, Vantiv, in its sole option, reserves the right to immediately terminate this Agreement and/or cease processing for the applicable Merchant locations upon notice to Merchant.

**7. Miscellaneous.**

This Merchant Services Agreement is entered into, governed by, and construed pursuant to the laws of the State of Ohio without regard to conflicts of law provisions. This Agreement may not be assigned by Merchant without the prior written consent of Vantiv. This Agreement shall be binding upon and inure to the benefit of the parties hereto and their respective successors, transferees and assignees. This Agreement is for the benefit of, and may be enforced only by, Vantiv and Merchant and is not for the benefit of, and may not be enforced by, any other party. Vantiv may amend this Merchant Services Agreement upon notice to Merchant in accordance with Vantiv's standard operating procedure. If any provision of this Agreement is determined to be illegal or invalid, such illegality or invalidity of that provision will not affect any of the remaining provisions and this Merchant Services Agreement will be construed as if such provision is not contained in the Agreement "Member Bank" as used in this Merchant Services Agreement shall mean a member of VISA, MasterCard and/or Discover, as applicable, that provides sponsorship services in connection with this Merchant Services Agreement. As of the commencement of this Merchant Services Agreement, Member Bank shall be Fifth Third Bank, an Ohio Banking Corporation, located at 38 Fountain Square Plaza, Cincinnati, OH 45263. The Member Bank is a party to this Merchant Services Agreement. The Member Bank may be changed, and its rights and obligations assigned to another party by Vantiv at any time without notice to Merchant.

IN WITNESS WHEREOF, this Merchant Services Agreement has been executed by the parties' authorized officers as of the dates set forth below.

| For My Payment Network, Inc: | | Pasco County Public Schools | |
|---|---|---|---|
| By: | _____ | By: | _____ |
| Name: | _____ | Name: | _____ |
| Title: | _____ | Title: | _____ |
| Date: | _____ | Date: | _____ |
| Address: | _____ | Address: | _____ |
| | _____ | | _____ |

Nicole Westmoreland 5.12.14

Signature Date

Nicole Westmoreland, MBA, Purchasing Agent
District School Board of Pasco County

MyPaymart NETWORK

# Appendix A
## Fees

The Customer agrees to pay the following fees. Customer authorizes the Service Provider's authorized agents to automatically take transaction fees directly from the Customer's bank account(s) that are registered with the Service and listed on any merchant applications signed by the Customer. Data Management fees shall be invoiced upon execution of the agreement.

Customer agrees to pay the monthly fee listed below. Customer agrees to pay the Set Up and Data Management fees listed below within 30 days of receiving the invoice.

| | |
|---|---|
| Set-up fee | $2,000 |
| Annual Fee | $1,400.00 |
| Transaction Fees | Based on the rates approved by the OCPS RFP1101024:<br>Cost plus .49% + $.10 per transaction for Visa, MasterCard, and Discover credit card transactions. |
| Monthly Fees | NA |
| Data Management Fees | Will be assessed if Pasco County needs these services |
| Training and Customer Support Costs | All inclusive in set up fees. No additional costs. |
| **Total Due at Signing** | **$2,000.00** |

CONTRACT REVIEWED AND APPROVED:
MW 5.12.14

MyPayment NETWORK

# Exhibit B

## PCI Security Policies

The following policies were developed by the United Compliance Framework to support merchants with best practices for complying with Payment Card Industry Data Security Standards. Each merchant accepting credit card for payment is expected to comply with best practices for maintaining data security.

**1.1 - Inventory and physically secure all media that stores confidential information**

- 1.1.1 - The organization must ensure all paper and electronic media that contains cardholder data are physically secured. Verify procedures exist for controlling physical access to paper and electronic media, including reports, faxes, CDs, disks, and hard drives.

**1.2 - Maintain media controls**

- 1.2.1 - Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data.
    - 1.2.1.1 - The organization must ensure all paper and electronic media that contains cardholder data are physically secured. Verify procedures exist for controlling physical access to paper and electronic media, including reports, faxes, CDs, disks, and hard drives.
    - 1.2.1.2 - The organization must ensure any media that contains cardholder data is strictly controlled during any distribution, either internally or externally. Verify a policy exists for the distribution of media containing cardholder data and that the policy covers the distribution to individuals in the organization.
        - 1.2.1.2.1 - The organization must ensure procedures are in place to have management approve any transit of sensitive media from a secured area.
        - 1.2.1.2.2 - The organization must maintain control over all media that contains cardholder data. Verify a policy exists for controlling the storage of media containing cardholder data.
        - 1.2.1.2.3 - The organization must ensure all media containing cardholder data is classified as confidential. Ensure all media containing sensitive information is labeled "Confidential."
        - 1.2.1.2.4 - The organization must ensure all media containing cardholder data can be tracked when being sent outside the facility. Ensure all media containing cardholder data that is sent outside the organization is authorized, logged, and tracked during transit.

**1.3 - Label media**

- 1.3.1 - The organization must ensure all media containing cardholder data is classified as confidential. Ensure all media containing sensitive information is labeled "Confidential."

**1.4 - Track while in transit**

- 1.4.1 - The organization must ensure all media containing cardholder data can be tracked when being sent outside the facility. Ensure all media containing cardholder data that is sent outside the organization is authorized, logged, and tracked during transit.

**1.5 - Obtain management approval for transit**

My Payment Network, Inc.
214 N. Hamilton Street, Ste. 102, Madison, WI 53703

CONTRACT REVIEWED AND APPROVED:
NW 5.12.14

- 1.5.1 - The organization must ensure procedures are in place to have management approve any transit of sensitive media from a secured area.

**1.6 - Physical protection while media is in storage**

- 1.6.1 - The organization must maintain control over all media that contains cardholder data. Verify a policy exists for controlling the storage of media containing cardholder data.

**1.7 - Manage disposition and destruction**

- 1.7.1 - The organization must ensure all cardholder data is destroyed when it is no longer needed. Verify the media destruction policy covers all types of media that contains cardholder data.
    - 1.7.1.1 - The organization will ensure that all hardcopy materials and media to be destroyed are done so in accordance with the strictest standards and guidelines.

**1.8 - Destruction and disposal of hard copy materials and media**

- 1.8.1 - The organization will ensure that all hardcopy materials and media to be destroyed are done so in accordance with the strictest standards and guidelines.

**1.9 - Management of third party services**

- 1.9.1 - The organization must ensure the service provider policies and procedures includes a list of all service providers, how the organization will monitor the compliance of the service provider with the PCI DSS requirements, and due diligence. Verify all third party service providers have policies and procedures in place requiring a list of all connected entities, performing due diligence prior to connecting the entities, verifying PCI DSS compliance, and for connecting and disconnecting entities.
    - 1.9.1.1 - Maintain a list of service providers. The testing procedures from Appendix A of this document should be performed to ensure the hosting providers are protecting the environment and cardholder data.
    - 1.9.1.2 - Establish processes and procedures for engaging service providers, including proper due diligence prior to engagement.
        - 1.9.1.2.1 - The organization must ensure a written agreement exists stating that the service provider is responsible for all cardholder data that the service provider possesses. Ensure all third party contracts contain a statement requiring the third party to acknowledge its responsibility for the security cardholder data it possesses.
            - 1.9.1.2.1.1 - Hosting providers must ensure the organization's environment and cardholder data that it is sharing is protected.
            - 1.9.1.2.1.2 - Shared hosting providers must ensure that only processes that have access to the cardholder data can be executed by that organization and that the organization's access and privileges are restricted to its own cardholder data environment. Verify if shared hosting providers are running their own applications, they are executed with the unique ID of the entity. Verify that any applications used by the hosting provider do not have a privileged user ID; the service provider has only read, write, or execute permissions for files it owns; the service provider's users do not have write access to shared binaries; logs only can be read by the owner of the information; and restrictions are in place for disk space, bandwidth, memory, and CPU usage.
        - 1.9.1.2.2 - Maintain a program to monitor service providers' compliance status.



CONTRACT REVIEWED AND APPROVED:
MW 5.12.14

- 1.9.1.3 - The organization will maintain a policy, standard, and procedure to select suppliers according to a fair and formal practice to ensure a viable best fit based on requirements.

**1.10 - Supplier Interfaces**

- 1.10.1 - Maintain a list of service providers. The testing procedures from Appendix A of this document should be performed to ensure the hosting providers are protecting the environment and cardholder data.

**1.11 - Acknowledgment of responsibility for data in possession and control**

- 1.11.1 - The organization must ensure a written agreement exists stating that the service provider is responsible for all cardholder data that the service provider possesses. Ensure all third party contracts contain a statement requiring the third party to acknowledge its responsibility for the security cardholder data it possesses.
    - 1.11.1.1 - Hosting providers must ensure the organization's environment and cardholder data that it is sharing is protected.
    - 1.11.1.2 - Shared hosting providers must ensure that only processes that have access to the cardholder data can be executed by that organization and that the organization's access and privileges are restricted to its own cardholder data environment. Verify if shared hosting providers are running their own applications, they are executed with the unique ID of the entity. Verify that any applications used by the hosting provider do not have a privileged user ID; the service provider has only read, write, or execute permissions for files it owns; the service provider's users do not have write access to shared binaries; logs only can be read by the owner of the information; and restrictions are in place for disk space, bandwidth, memory, and CPU usage.

**1.12 - Formalize third party relationships**

- 1.12.1 - Establish processes and procedures for engaging service providers, including proper due diligence prior to engagement.
    - 1.12.1.1 - The organization must ensure a written agreement exists stating that the service provider is responsible for all cardholder data that the service provider possesses. Ensure all third party contracts contain a statement requiring the third party to acknowledge its responsibility for the security cardholder data it possesses.
        - 1.12.1.1.1 - Hosting providers must ensure the organization's environment and cardholder data that it is sharing is protected.
        - 1.12.1.1.2 - Shared hosting providers must ensure that only processes that have access to the cardholder data can be executed by that organization and that the organization's access and privileges are restricted to its own cardholder data environment. Verify if shared hosting providers are running their own applications, they are executed with the unique ID of the entity. Verify that any applications used by the hosting provider do not have a privileged user ID; the service provider has only read, write, or execute permissions for files it owns; the service provider's users do not have write access to shared binaries; logs only can be read by the owner of the information; and restrictions are in place for disk space, bandwidth, memory, and CPU usage.
    - 1.12.1.2 - Maintain a program to monitor service providers' compliance status.

**1.13 - Audit provisions**

- 3.13.1 - Maintain a program to monitor service providers' compliance status.

**2.0 Enforcement**

CONTRACT REVIEWED AND APPR
MW 5.12.14

MyPayment NETWORK

Failure to comply with the policies outlined above may result in a failure of the companies PCI compliance and may result in penalties up to termination of the offending employee.

Policies provided by UCF

The Unified Compliance Framework is the first independent initiative to exclusively support IT compliance management by focusing on commonalities across regulations, standards-based development, and simplified architectures. Unified Compliance's strategic approach to IT compliance reduces cost and limits liability. The UCF's strategic approach simplifies compliance and standards, reduces cost, limits liability, and leverages the value of compliance-related technologies through a harmonized set of controls against which all regulatory standards and best practices can be mapped.

The UCF was created by Dorian Cougias and his research partner, Marcelo Halpern of the international law firm Latham and Watkins, which oversees all legal aspects of the UCF.

**Merchant Signature acknowledges you have read the best practices for complying with payment card industry standards for maintaining data security and will incorporate practices into your operations for managing and working with cardholder data.**

_____
Initials

_____
Date

CONTRACT REVIEWED AND APPROVED:
NW 5.12.14

My Payment Network, Inc.
214 N. Hamilton Street, Ste. 102, Madison, WI 53703

# SchoolPay® Security Policy

SchoolPay delivers online payment services to schools in the United States. Due to the nature of our business – making online payment fast and easy for schools – security is an important part of what we do. There are several aspects to our security which are outlined below. If you require additional information about SchoolPay's security please send an email to customerservice@schoolpay.com.

## Physical Secure Hosting

The SchoolPay service runs on servers that are hosted by a large, national private hosting company that provides state-of-the-art security. The servers are located in a facility with several layers of physical security, including alarms, and video surveillance.

## Secure Sessions and Intrusion Detection

All SchoolPay user sessions and payment sessions are encrypted. The flow of data between the user's computer (or device) and SchoolPay servers is encrypted with SSL security. SchoolPay maintains security certificates with nationally known firms. Further, SchoolPay uses Intrusion Detection systems to detect attempts to "hack" into the SchoolPay system. Any suspected "hacking" attempt results in the session being terminated.

## Hosting Firewall

SchoolPay user sessions are protected by multiple firewalls. There are firewalls between the web servers and the internet. Once within the SchoolPay service there are firewalls between the database and the web servers.

## Encrypted Database

The SchoolPay databases are encrypted. This means that if a "hacker" was able to get past the intrusion detection and the firewalls the data in the database would be scrambled. The keys used to decrypt the data are stored, offsite at a third-party company and leader in secure key storage and usage.

## PCI-DSS and Intrusion Audit

SchoolPay is audited, annually, by a Qualified Security Assessor (QSA). QSA's are independent audit firms, authorized by the Payment Card Industry, to assess all aspects of software and business operations to confirm it meets or exceed every aspect of Payment Card Industry Data Security Standards (PCI-DSS). In addition, SchoolPay undergoes daily security scans, and annual, third-party external testing of our ability to terminate any hacking or SQL injection attempt.