

Sample Letter - please note any dates referenced in this letter are for sample purposes only

Dear Valued Merchant:

Thank you for choosing InterceptEFT for your payment processing needs. We value your business and want to continue helping you realize the benefits of our relationship. Part of our commitment is to inform you of changes that may affect your merchant account, including updates to your fees and the requirement of all merchants to maintain Payment Card Industry (PCI) Data Security Standards (DSS) compliance. Please take a moment to read this entire letter to learn more about **our PCI Compliance Assistance Service Program, new applicable fees and how you can minimize your costs and risks by becoming PCI DSS compliant.**

PCI DSS Compliance Requirement

The payment brands (American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.) have mandated that all merchants who store, transmit or process cardholder information must maintain compliance with the PCI DSS. We, as your service provider, take the protection of customer and payment account data very seriously. We understand the risks and financial costs that a compromise can pose to your business. In support of this important mandate, we will begin requiring all of our merchants to validate their PCI DSS compliance status with us. However, we want to make the process as convenient as possible for you.

Our Compliance Assistance Service Program

InterceptEFT has established a relationship with SecurityMetrics, a leading provider of PCI audit and scan services. They are certified by the PCI Security Council as a Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV). Enrolling with SecurityMetrics will provide you with access to trained professionals to help your business comply with the PCI DSS. They will work with you to conduct an analysis of your account, assist with any necessary remediation efforts and help you certify your compliance. The service will guide you through the completion of your PCI DSS Self-Assessment Questionnaire (SAQ) and includes (if applicable) the required quarterly scans of your processing systems. To learn more about SecurityMetrics and to initiate an analysis of your account, please choose from one of the following enrollment options:

Online: www.securitymetrics.com

Fax: see the enclosed *PCI Enrollment Data Sheet*

Mail: see the enclosed *PCI Enrollment Data Sheet*

Phone: call SecurityMetrics toll-free at (800) 557-4684

Notes:

When prompted for your “Acquiring Bank or Merchant Processor”, please select “InterceptEFT”

When asked for the last 6 digits of your merchant number, please reference the merchant number listed at the top of this letter

Once your account is certified, SecurityMetrics will complete the validation process for you by notifying us of your compliance.

Applicable Fees

Effective September 30, 2009, your merchant agreement will be amended to include the following fees:

a \$79 Compliance Service Fee will be added to your InterceptEFT merchant account. This fee will be charged annually on or after September 1. This fee will allow us to continue providing you high level support with respect to compliance standards put forth by the payment brands, the PCI Security Council and various government entities. As part of this fee, the SecurityMetrics services described above will be provided to you at no additional charge.

a \$19.95 monthly Non-Receipt of PCI Validation Fee that may be billed in any given month your account is deemed non-compliant with the PCI DSS. To allow you time to complete the PCI DSS certification process, this fee will not be added to your account until December 25, 2009. If we do not receive validation of your compliance by December 25, 2009 your account will be billed \$19.95 on your December month-end statement and in each month thereafter until we receive the required validation. Please note that you must maintain PCI compliance at all times and recertify your compliance annually (or quarterly, if applicable) in order to avoid this fee in the future. In addition, we reserve all of our rights under the merchant agreement including, but not limited to, terminating your services for non-compliance with association rules and regulations.

Maintaining your merchant account with us or use of your merchant account on or after September 30, 2009 will represent your acceptance of these terms.

While participation in the PCI Compliance Service Assistance Program helps to mitigate the risk of a security breach or data compromise, participation does not guarantee or prevent a security breach or compromise.

We appreciate your business and understand that you may have questions. For additional information, the follow reference materials have been enclosed:

A list of Frequently Asked Questions regarding PCI DSS

The SecurityMetrics PCI Enrollment Data Sheet

If you still have questions, we encourage you to contact our Customer Service Department at the phone number printed on your merchant statement for additional information.

Sincerely,
InterceptEFT

PCI Compliance Validation Service Program

Frequently Asked Questions

What is PCI DSS?

The Payment Card Industry (PCI) Data Security Standard (DSS) is a set of requirements for enhancing payment account data security. These standards were developed by the PCI Security Standards Council, which was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa, Inc. to facilitate industry-wide adoption of consistent data security measures on a global basis. The standard aims to increase awareness and promote best practices in the handling of sensitive information as a means to minimizing identity theft and fraudulent transactions.

Is PCI DSS new?

No. The framework of the PCI data security standards has existed in different forms for some time now and continues to evolve. You may be more familiar with the payment brands' programs that promote the adoption of the PCI DSS

MasterCard: Site Data Protection (SDP)
program ○ [Mastercard.com/sdp](https://www.mastercard.com/sdp)

Visa: Cardholder Information Security Program
(CISP) ○ [Visa.com/cisp](https://www.visa.com/cisp)

Discover Network: Discover Information Security & Compliance (DISC)
○ [Discovernetwork.com/fraudsecurity/disc.html](https://www.discovernetwork.com/fraudsecurity/disc.html)

American Express: Data Security Operating Policy
○ [AmericanExpress.com/datasecurity](https://www.americanexpress.com/datasecurity)

I only process a few hundred dollars a month. Does my merchant account still need to be PCI compliant?

Yes, all merchants, whether small or large, are required to be PCI compliant. The payment brands have collectively mandated PCI DSS compliance for any and all organizations that process, store or transmit payment cardholder data. Inherent in having a merchant account is the ability to handle cardholder data.

I already use a "PCI compliant" terminal/gateway. Doesn't that mean I am PCI compliant?

No. Use of a PCI compliant payment application is one aspect of the many PCI DSS requirements, which cover handling of sensitive data. Currently, the PCI DSS lists twelve requirements. These requirements are organized around the following principles:

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

Can I choose not to certify for PCI compliance?

If you choose not to complete the self-assessment questionnaire (and applicable network scans) you may overlook certain data security practices that minimize your risk of a security breach. In the event that your business is compromised, you may be subject to substantial fines per payment brand. These fines would be in addition to the expenses and fraudulent transactions resulting from the breach.

In light of the importance that data security has to the payment processing industry and consumers at large, we, as your service provider, may also begin imposing a fee for each month that your account has not been validated as PCI compliant or in any given month your account is deemed non-compliant. Failure to validate compliance may result in the termination of your merchant account.

What do I need to do to validate my PCI DSS compliance?

We have established a relationship with SecurityMetrics, Inc., a leading provider of PCI audit and scan services. SecurityMetrics' service includes: assistance in determining which version of the Self-Assessment Questionnaire is appropriate for your business; administration of any applicable network scans; guidance on any necessary remediation efforts; and certification and validation of your account's compliance. These SecurityMetrics services are available to you as part of our *PCI Compliance Assistance Service Program*. You can take advantage of this opportunity by enrolling with SecurityMetrics via their Web site securitymetrics.com or by calling (800) 557-4684.

How long is the PCI compliance certification valid?

The PCI compliance certificate is valid for one year from the date the certificate is issued. To maintain your compliance, you are required to complete the PCI DSS self-assessment questionnaire annually and conduct any applicable network scan on a quarterly basis.

Do I have to use SecurityMetrics?

No. There are more than 130 qualified security assessors and approved scanning vendors. You are free to choose to certify with any vendor you like. However, if you choose to certify with another vendor you will be responsible for paying the full cost of the PCI Compliance analysis to that vendor. A list of approved vendors is available on the card association web site or at pcisecuritystandards.org.

What if I have already been certified or choose to certify through another Qualified Security Assessor (QSA)/Approved Scanning Vendor (ASV)?

If you have already been PCI DSS certified or if you choose to use another QSA/ASV, please submit your certification documentation to us via e-mail at pci.1@firstdata.com or fax to (402) 916-8240.