



VeriFone Payment System Security Best Practices

© Copyright, 2007, VeriFone

The following text is protected by law from any form of duplication unless prior permission is obtained from the officers of the aforementioned company.

Introduction

Look no further than to recent news headlines about security breaches and data compromises involving merchants of all sizes and you'll see the criminal element is taking more risks, yet achieving success with more regularity. And, whether it's fair or not, the 'fault' of these attacks is increasingly placed squarely on the shoulders of merchants and system integrators. If you are a merchant and, there are many safeguards that must be in place to ensure you are compliant with the most recent interchange initiatives and, more importantly, you are well protected in case of a breach.

This document analyzes the Best Practices for Payment System from a sound security perspective to minimize fraud. The intended audience is merchants and system integrators who utilize a payment software solution via either a POS product or virtual terminal. While the list of best practices we provide in the following document is a great start to protect your business, it is by no means a "be all, end all". We strongly encourage all merchants and system integrators to review the references we provide in Section 3 for more information and to make special attention to the fraud prevention information provided by the major card associations and the Payment Card Industry (PCI) Security Standards Council.

Best Practices – Payment System Security

1. Ensure that your integrator has implemented the payment system according to PCI guidelines. Additionally, ensure that you POS vendor received recent validation from a certified application security assessor and will continue to do so regularly. Finally, make sure that the payment processing software being implemented has current PABP (Payment Application Best Practices) validation.



2. Once implemented, make sure that credit card magnetic stripe data, expiration dates and CVV2/CVC2/CID data (the verification number that appears on the front or back of the credit card) is never stored by the payment system. VeriFone's software solutions are designed to eliminate the need to store this data. After completion, each transaction is assigned a unique identification number called a TROUTD. Merchants can use each TROUTD as a key to reference the transaction associated with this data safely and securely.
3. Control and limit access, via unique usernames and passwords, to the payment system. Regularly change usernames and passwords and quickly revoke any that were used by employees who leave the company. Additionally, any and all encryption keys utilized in the payment system at least once a year.
4. Use appropriate facility entry controls to limit physical access to the hardware which hosts the payment system. Printed material documenting sensitive merchant information (Merchant ID, Terminal ID, etc.) should also be safeguarded by setting appropriate limits on its access.
5. Track and monitor all access to payment systems with the use of audit logs. This includes successful and unsuccessful login attempts, root/administration access, and even access to the audit logs themselves. Regularly back-up, secure and retain these logs for at least three months online and one year offline.
6. If the PC or server running a payment application is on a network that has a dial-up or high-speed Internet connection, a firewall must be used on that network. Once a firewall is in place, ensure that all available security patches have been installed. Perimeter scans and intrusion detection are also recommended.
7. Keep all relevant software associated with the payment system up to date including, but not limited to: operating systems, e-mail programs and Internet browsers.
8. If the integrated merchant application is designed to allow remote software updates, the communication methods used to provide those updates must be PCI compliant. If modems are used to communicate updates, they should be turned on only for that purpose and immediately turned off. For "always-on" high-speed connections, firewalls must be properly configured to secure these connections.
9. If the integrated merchant application allows administration from internal systems, access must be secured by the use of encrypted protocols such as Transport Layer Security (TLS) or Secure Shell (SSH). Telnet or rlogins must never be used for administration.
10. If the payment system utilizes a wireless network, validate that the wireless entry point(s) have been properly configured. Ensure a firewall is in place and regularly scan the wireless network for unauthorized wireless signals.

References

1. VeriFone Secure Retail Payments Web Portal
 - <http://www.secureretailpayments.com>
2. VeriFone Security and Mandates Information Web Page
 - <http://www.verifone.com/industry/security/index.html>
3. Payment Card Industry (PCI) Data Security Standard
 - <https://www.pcisecuritystandards.org>
4. Visa Cardholder Information Security Program (CISP)
 - http://usa.visa.com/merchants/risk_management/cisp.html
5. American Express Fraud Prevention for Merchants
 - https://home.americanexpress.com/homepage/merchant_ne.shtml
6. MasterCard Site Data Protection (SDP) Program
 - <http://www.mastercard.com/us/sdp/index.html>
7. Discover Information Security and Compliance Program (DISC)
 - http://www.discovernetwork.com/merchant/resources/data/data_security.html

About VeriFone Software Solutions

VeriFone is recognized worldwide as the leading provider of secure electronic payment technologies. Thousands of customers count on our PABP (Payment Application Best Practices) validated software solutions and unequalled professional support services to drive business success. Our software solutions enable our partners and customers to accept fast, secure electronic payments from their customers wherever, whenever, and however transactions occur.

With today's complex customer needs and changing payment security requirements, VeriFone has the unrivaled infrastructure, expertise and experience to help integrators and merchants successfully implement any payment solution. VeriFone continually evolves and invests in its payment software solutions to keep up with security standards and mandates. VeriFone also works with our customers to fine-tune our solutions to their unique market requirements, and the result is an offering of secure, interoperable solutions for a vast array of applications and transaction environments.



If you are not a VeriFone customer, contact us today and let our industry experts help you get started. We can provide you with everything from educational materials and resources all the way to a detailed software solution migration plan to get you up to speed and ensure you meet industry compliance. We've helped thousands of companies securely and successfully process billions of transactions and protect their customers' data, and we can help you too.

Contact Information:

VeriFone Software Solutions
8001 Chatham Center Drive, Suite 500
Savannah, GA 31405
Phone: (800) 725-9264
Email: SalesInfo@verifone.com
Website: www.verifone.com

