



ICVERIFY, Inc. Secure Software Guide

March 15, 2007

The information contained herein is intended to apply to the Visa[®] and MasterCard[®] data security regulations and guidelines in effect as of April 1, 2005. However, those regulations and guidelines are subject to change at any time, and new standards may come into existence at any time. Therefore, ICVERIFY, Inc. encourages you to work with Visa[®] and MasterCard[®] and your merchant bank on a regular basis to ensure your compliance with all applicable data security standards.

Overview

Thank you for purchasing an ICVERIFY, Inc. software product. We value your purchase and want to share important information with you regarding installing and operating your software in a way that is consistent with the security guidelines of the payment processing business.

Security of cardholder information is of critical importance to everyone involved in the acceptance of card payments. As part of a continuing effort to keep you aware of the requirements for securing cardholder data, we are providing you with additional information to help you to understand the data security standards being produced by Visa[®] and MasterCard[®].

Understanding the Importance of the Data Storage Regulations

The first part of operating under these standards is to understand the importance of data security and how it affects you and your customers. The rising incidence of cardholder data theft results in financial losses and additional operating expenses and significant inconvenience and personal losses to the consumers. The Visa[®] and MasterCard[®] regulations address additional security requirements that can result in sizeable fines arising from not adhering to the guidelines. Data security is vital for the protection of your customers and it can also have a significant effect on your bottom line.

IMPORTANT NOTE: You may have a direct obligation as a merchant to demonstrate compliance with the data security programs operated by the card associations. If you have not done so already, you must review the data security standards available at the credit card companies' Web sites. A list of links is provided at the end of this guide. At the very least, you should download and complete the *PCI Self-Assessment Questionnaire* as an internal exercise to judge your own security standards.

**Our
Responsibilities
as Your
Software
Provider**

It is important to understand that the card associations' compliance programs governing data security, generally referred to as the *Payment Card Industry* (PCI) standards, are aimed at entities that **receive, store or transmit** payment information. This means they apply, for example, to **merchants** and **service providers** (like gateways and processing companies), but **not** to software providers like ICVERIFY, Inc. A separate program called the *Payment Application Best Practices* (PABP) applies to software providers; this is discussed in detail in the next section.

This is a very important distinction to make because while you can enjoy the confidence and security of using a PABP-accredited software application, you still have an obligation as a payment acceptor to demonstrate your compliance with the applicable assessment program for your business.

However, ICVERIFY, Inc. can assist in your compliance effort by confirming that our latest software releases meet current standards in that they do not store the following critical card data elements subsequent to authorization:

- Full track data from a card's magnetic stripe
- CVV2, CVC2 and CID numbers from the physical card
- PIN block data from PIN-based Debit transactions

Furthermore, the software contained on your CD-ROM protects all stored transaction data with *strong encryption*, which is defined as using an industry-standard technology such as 3DES or AES with a cipher of 128 bits or greater. In the case of ICVERIFY, Inc.'s product line, 256-bit AES is used to protect data such as the following:

- Transaction amounts, approval codes and payment card numbers
- Customer names and billing/shipping addresses
- Other identifying information, such as applicant employment information used in line-of-credit application processing

Please refer to the *Data Storage Statement* located on your software installation CD-ROM, or available at <http://www.icverify.com>, for specific information.

**The Payment
Acceptance
Best Practices
(PABP)
Program**

At the end of 2004, Visa[®] acknowledged the need for a separate validation program for software providers and created the Payment Application Best Practices. The PABP are a currently voluntary set of guidelines that address the design and implementation of payment processing software. You can examine the latest distribution of the PABP documentation by following the links for Payment Applications at <http://www.visa.com/cisp>.

In February 2005, the PABP guidelines for software providers were aligned with the joint Payment Card Industry (PCI) standards for merchants. This makes it easier for merchants to understand the relationship between the software they use and their own compliance responsibilities, as more software providers become PABP-validated in the coming months and years.

Although the PABP guidelines are currently voluntary, ICVERIFY, Inc. is proud to announce that both ICVERIFY™ for Windows™, version 4.0 and later, and ICVERIFY Enterprise Edition, version 1.5 and later, conform fully to the PABP standards that were publicly available as of the version release date. We also perform routine audits of our products with an external security assessor to confirm their ongoing conformance to the standards, as they occasionally evolve and change.

At the conclusion of each product audit, a full security report is delivered to Visa for their review and acceptance. When the review process is complete, Visa issues PABP accreditation for the product and version reviewed.

You can download copies of our PABP acceptance letters at the ICVERIFY, Inc. Web site at <http://www.icverify.com>.

Part of the PABP program obligates us as a software vendor to produce documentation to help you understand how your copy of ICVERIFY, Inc. software relates to your payment processing operations, and your obligations under the various compliance programs. We hope this document will be valuable to you in that regard.

**What's
Important to
Know about
Your Payment
Processing
Software**

ICVERIFY, Inc.'s products can be used in two ways – either as stand-alone, turnkey payment applications, or components of a larger payment acceptance system such as an electronic cash register, Web site, or order entry system. Your data security obligations as a merchant extend to the payment acceptance system *in its entirety*. For example:

- If you created a custom interface to your ICVERIFY, Inc. product, you need to assess the data security standards of your own software code and computer infrastructure.
- If you purchased an ICVERIFY, Inc. product from a systems integrator, you need to retrieve information from the integrator about the **entire system**, not just from ICVERIFY, Inc.
- The security of your computer equipment is just as critical as that of your ICVERIFY software product. The most secure product in the world will not be effective if you do not secure the equipment on which it runs.

It's important for you to conduct a thorough assessment because you may be required to make representations to your merchant bank, as well as the card associations, about your entire payment system. ICVERIFY, Inc. can only furnish information about its own products, not your entire system.

**General
Notes for All
Merchants**

As stated earlier, it is critical for you to bear in mind that your obligation to protect consumer data does not end with your ICVERIFY, Inc. product, even though it is fully PABP-validated. You have an ongoing responsibility to your merchant bank, and indeed to your customers, to treat their data with care. ICVERIFY, Inc. recommends instituting at least those practices listed on the following pages, regardless of how you use your software.

IMPORTANT NOTE: ICVERIFY, Inc. encourages you to develop, and Visa® and MasterCard® may require that you develop, additional safeguards, so please be sure to periodically verify with those associations and your merchant bank that you are complying with all applicable data security regulations and guidelines.

**Stay Current
With Your
Equipment**

Both hardware and software manufacturers occasionally publish updates to their products to take advantage of changes in the market, or to protect against emerging threats. You should routinely check whether updates are available for any of your other computer equipment, for example by reviewing manufacturer Web sites, newsletters, support groups, and so on. Updates may take the form of driver downloads, physical components and the like.

On occasion, a software or hardware manufacturer may withdraw support for a product altogether. If this happens, consider what the exposure to your business might be if you continue using an unsupported product.

It's also possible that a manufacturer may alert you to a flaw in a product that exposes your company to security risks. *Take these alerts very seriously.* Do not assume that you can safely use compromised products just because your business may be small or only known in your local area. Hackers intentionally target smaller businesses because they assume they are less sophisticated, and therefore easier prey, than larger ones.

**Applicable Law
and the
“Golden Rule”**

Although one of your foremost obligations is to demonstrate compliance with the PCI standards, you may be subject to local, state or federal regulations governing privacy and consumer data protection. Be aware of the applicable laws for your location and line of business, as well as the “golden rule” standard of data protection. Don't just comply with the law – ask yourself how you would want your own information to be treated and perform your business accordingly.

**Product,
System and
Device
Passwords**

Effective use of passwords is one of the easiest and most effective measures you can take to safeguard your systems and data.

- **Product Passwords.** Secure your ICVERIFY, Inc. product by means of the ICVERIFY User Manager. Require your computer users to log in using a complex password (a password of sufficient length containing both letters and numbers in it). As an added security measure, consider using the password-expiration feature in the User Manager to force users to change their passwords routinely – for example every 30 or 90 days. Review the section entitled [Complex Passwords](#) for additional information.
- **Computer Passwords.** After securing the product itself, lock down the PC on which the product resides. Use the built-in strong security features of the Microsoft® Windows® operating system to require your users to log in, also using a complex password if possible. Again consider forcing users to change their passwords on a routine schedule.
- **Device Passwords.** Network devices like routers, proxy servers and firewalls can provide excellent protection, but if you leave them with their default settings intact, they may be virtually useless. Don't leave any administrator-level passwords in their default configuration – change them to a complex password that only you know. Complex passwords will be much more difficult for a malicious user to guess. Likewise, don't leave access control lists or device logins at their default (usually open) setting. This makes it far too easy for malicious users to attach devices or other computers to your network, browse your own computers, and look for sensitive data to harvest.

If you are uncertain what a complex password is or need help thinking of one, review the section entitled [Complex Passwords](#) for additional information.

Complex Passwords

A complex password is a password that contains both alphabetical and numeric values. The following are examples of complex passwords:

red4balloon5
rome0andjulie8
auth3nt1cate

It is much more difficult for a malicious user to guess a complex password than a password that is all letters. You may also notice the final example (auth3nt1cate) replaces the letters *e* and *i* with digits. Consider where you can add digits either in addition to, or instead of, the alphabetical characters in a password to increase its security.

Since complex passwords are a PABP requirement, you will find the ICVERIFY User Manager enforces them, and you will not be able to set up or access a user account without one.

Try to train yourself and your users to utilize complex passwords wherever possible. The PABP standards require you to use them to access the ICVERIFY software products; you should consider enforcing them for other password-protected facilities within your environment, such as network access, Internet router access, mainframe logins, etc. Depending on your processing volume and line of business, you may be required to secure any computers or network devices used to process or transmit payment transactions using complex passwords. Therefore, it is best to get into the habit of using them.

Network Security

Now that you have implemented passwords to protect against internal attacks, consider the security of your network from unwelcome access, whether internal or external.

- **Network Security.** *Never* install a payment software application on a computer with a direct link to the Internet unless that link is secured. If you are using the Internet for your transaction transport, make sure your Internet hardware (cable modem, DSL router, etc.) has built-in firewall capabilities. Take advantage of the built-in Windows Firewall application and restrict access to the computer on which your ICVERIFY product is running to only the protocols and routes needed for the software to function:
 - If you're running an ICVERIFY product on a single computer connected to an Internet connection of some type, allow only the protocol required by your processor (typically HTTP or TCP) and only to the IP address or URL supplied by that processor. Disallow all other protocols through the firewall for maximum protection.
 - If you're running an ICVERIFY product on multiple computers tied together in a logical network, make sure that any other protocols required by your server or master station (for example Named Pipes) are only allowed from the specific computers running the software.

Always practice good firewall management. If you need to open your firewall to allow a particular type of protocol or connection for your software to function, don't allow that connection to the entire world. Try to restrict access only to those machines or devices you know and trust. *Don't surf the Internet with the computer you use to process payments!*

- **Wireless Devices.** Your ICVERIFY, Inc. product has been designed to work on any network that supports TCP/IP protocols, without direct knowledge of the physical devices or communication technologies underlying the TCP/IP layer. If you use wireless devices of any kind to store or transmit payment transaction data, those devices must be configured to encrypt transmissions using technologies consistent with the standards in the *Payment Card Industry* guidelines. *Note:* Security issues have been found with the WEP Wireless Encryption Protocol. It is strongly recommended that you implement additional security measures on top of WEP, such as IPsec or SSL.
- **Remote Access.** ICVERIFY, Inc. does not perform remote access operations and does not test with remote access software. If you use any remote access software to manage the computer on which your ICVERIFY, Inc. product is installed, it is your responsibility to configure and operate that software in a manner consistent with the *Payment Card Industry* guidelines.

**Access and
Data
Restriction**

Restricting logins and protecting against attacks are both important. You should also think about what kind of information your legitimate users truly need to access, how long you should retain it, and how to restrict their access to data they do not need to perform their jobs.

- **User Security.** Your ICVERIFY, Inc. software product allows you to “lock down” access to only those users with a legitimate need to use it. Familiarize yourself with the capabilities of the **ICVERIFY User Manager** application so that you can assign usage profiles, create users and manage user passwords effectively. Please read the *ICVERIFY User Manager Guide* for important information on how to set up and configure user account security for your application. Follow the simple rule of thumb that users should not be granted a particular privilege unless there is a legitimate need for them to use it.

For example, a “Clerk” may only facilitate sales and therefore would not need to have access to the Credit and Reporting functions. In this scenario, you could create two profiles called “Clerk” and “Supervisor” and ensure that only members of the “Supervisor” profile can perform Credits and generate reports.

- **Retention and Protection of Data.** Your ICVERIFY, Inc. product allows you to store transaction data for a very long time. This is important to some merchants; however, ask yourself how long you really need to retain your transaction data. Develop a schedule for deleting or destroying data once you are certain you no longer need it. This destruction policy should extend to physical transaction information as well. Once you have established your policy, update the storage parameters in your software to be consistent with the policy. Consult the user manuals for your particular product for further information.
- **Access to Information Outside the Product.** If you use the transaction export or import features, or if you have integrated your ICVERIFY software product with another system, you must take steps to secure any transaction information outside the product – for example, the source application you used to import data, or the target application you use to receive data. If the programs or processes you use to manage data outside the ICVERIFY product itself are not secure, a malicious user may simply bypass the product and attack the weakest link in your payment acceptance process. Don't let this happen. Examine all points of your process for appropriate access and controls. Bear in mind that data security outside the product is entirely your responsibility, not that of ICVERIFY, Inc.
- **Encryption Keys.** Your ICVERIFY software product allows you to regenerate data encryption keys on demand. Consult the *User Guide* for your product on the specific steps required to perform this function. ICVERIFY, Inc. recommends that you regenerate your encryption keys at least once a year, whether or not you have suffered a security issue.

**How ICVERIFY
Products Use
the Internet**

Your ICVERIFY software product supports transaction processing over the Internet. Every connection made with a processing network over the Internet is secured by means of 128-bit SSL or stronger encryption. This encryption happens automatically by your software and is tested as part of the certification of the software by ICVERIFY, Inc. and our processing partners.

**Stay Current
on Patches**

ICVERIFY, Inc.'s products can be used in two ways – either as stand-alone, turnkey payment applications, or components of a larger payment acceptance system such as an electronic cash register, Web site, or order entry system. Your data security obligations as a merchant extend to the payment acceptance system *in its entirety*. For example:

- If you created a custom interface to your ICVERIFY, Inc. product, you need to assess the data security standards of your own software code and computer infrastructure.
- If you purchased an ICVERIFY, Inc. product from a systems integrator, you need to retrieve information from the integrator about the **entire system**, not just from ICVERIFY, Inc.
- The security of your computer equipment is just as critical as that of your ICVERIFY software product. The most secure product in the world will not be effective if you do not secure the equipment on which it runs.

It's important for you to conduct a thorough assessment because you may be required to make representations to your merchant bank, as well as the card associations, about your entire payment system. ICVERIFY, Inc. can only furnish information about its own products, not your entire system.

**General
Recommendations
(Continued)**

- **Other Software.** Evaluate the computer on which your ICVERIFY, Inc. product is installed. If other software applications that potentially represent a security risk are present on the system, such as remote-access software, consider removing them or locking them down to reduce the risk of malicious use. Limit or remove the file- and directory-sharing capabilities of the operating system. Disable or uninstall unused software, devices and drivers.
- **External Review.** Depending on the amount of card transactions you process, you may be obligated to engage an external security assessment company to judge your level of compliance with the various security compliance programs. If you choose to follow this path, consider engaging a CISP-qualified assessor who is versed in the latest requirements from the card associations. Remember, cardholder security is a rapidly changing subject and the standards can change.
- **User Security.** Your ICVERIFY, Inc. software product allows you to “lock down” access to only those users with a legitimate need to use it. Familiarize yourself with the capabilities of the **ICVERIFY User Manager** application so that you can assign usage profiles, create users and manage user passwords effectively. Please read the *ICVERIFY User Manager Guide* for important information on how to set up and configure user account security for your application. Follow the simple rule of thumb that users should not be granted a particular privilege unless there is a legitimate need for them to use it.
- **Internet Transport Security.** As discussed earlier, if you use the Internet to transmit payment transactions to your processor network, it is essential that you implement a firewall to protect your computer(s) from Internet-based attacks. This is especially important if you are running an ICVERIFY product on a computer that has direct access to your Internet connection (for example, if you have only one PC and that PC has a dial-up, cable or DSL modem attached to it.) Remember also that the ICVERIFY Internet communication application called JCard can be installed on a separate computer from the main ICVERIFY software, if you want to have physical segregation of your payment application and Internet transport service. Consult the installation materials that came with your software for options.
- **Industry Best Practices.** ICVERIFY, Inc. recommends you evaluate your payment processing operations in the context of the comprehensive security guidelines published by the Open Web Application Security Project. You can download and review their documentation for free at <http://www.owasp.org>.

**Special Note
for Merchants
Using a Third-
Party
Integration**

As discussed earlier, many merchants use an ICVERIFY, Inc. product as one part of an integrated payment processing system. If you are such a merchant, it is important that you secure certain important information from your integration partner. ICVERIFY, Inc. is continually working with our integrator community to ensure they are aware of security and compliance trends in the payments industry; however, since you, as a merchant, are under a special obligation to represent to your merchant acquiring bank that you are processing transactions securely, you should engage your integrator on your own initiative. The information you need to determine includes the following items. Ask your integrator for the following information, regardless of the type of ICVERIFY, Inc. product you are using:

- **ICVERIFY, Inc. Product and Version Used.** Your integrator should be able to tell you the exact ICVERIFY, Inc. product and version number embedded in your payment system. Ideally, it should be a product and version listed on the first page of the *Data Storage Statement* located on your installation CD-ROM. If it is not, please ask the integrator to contact ICVERIFY, Inc. at (800) 538-0651 or by e-mail at sales-icv@icverify.com to discuss upgrading its ICVERIFY, Inc. product integration.
- **Software Integration Method Used.** Once you have established your integrator's choice of product and version, your integrator needs to confirm that the integration method used is currently supported and conforms to the recommendations laid out in this document. If your integrator is using an integration method designed for a product that is no longer supported, such as ICVERIFY™ for MS-DOS™ or PCAuthorize™, the integration will need to be updated. ICVERIFY, Inc. encourages you to share this document with your integrator and to involve us in any discussions as you deem appropriate.
- **Assessment of All System Components.** Remember, your integrator may have chosen an ICVERIFY, Inc. product as the core payment processing engine for your payment system, but the integrator has the same responsibility to demonstrate compliance with data storage rules as ICVERIFY, Inc. does. Ask for any relevant documentation or procedures detailing how to install, secure and operate all relevant parts of your integrator's payment system. Pay close attention to any components that store or manage customer data, including customer databases for loyalty or recurring billing, system activity logs, and reporting systems to determine their level of adherence to current standards.

**Special Note
for Merchants
Using the
ICVERIFY
Master / Sub-
Station Mode**

The ICVERIFY for Windows product can be networked in what is commonly called "Master / Substation mode," where the substations route transactions to the master station to forward on to the processing network. This mode uses either the built-in request-answer shared-directory method to communicate between the stations, or the Microsoft Message Queue (MSMQ) subsystem, depending on the operating system you use. In either case, transactions are fully encrypted between stations; however, the substations need file-level network access to the master station to perform other application functions.

Therefore, if you use this mode to process your transactions, you need to follow the same guidelines as merchants who use the shared-directory method for their own software integrations:

- **Network Permissions.** The master station and substations must all have the appropriate permissions to the shared directory so that the request and response transactions may be properly cleaned up when the transaction is complete. Ensure that the master station and all substation computers have full "read/write/delete" permissions to the shared folder.
- **Network Security.** Ensure the file transmissions between the master station and the substation computers are adequately secured, especially if the stations interact over a wide-area network or VPN.
- **User and Password Protection.** As discussed in the General Note to All Merchants, ICVERIFY strongly recommends that you implement a strong user management model for your payment application. Since you are running the ICVERIFY software in a distributed environment, it is especially important for you to consider the security of all the computers processing payment transactions rather than just one.

**Special Note
for Merchants
Using the
ICVERIFY
Request-
Answer
Interface**

Many merchants have used the ICVERIFY “request-answer” software interface, commonly referred to as the ICVERIFY SDK, as a simple way to perform transaction processing. You can use the request-answer interface with confidence within these guidelines:

General Note for all SDK users – “Secure Deletion”:

- Review your integration to determine whether you are practicing “secure deletion” of data. Secure deletion means that before discarding potentially sensitive data, you are rendering it unreadable or unusable. For example, if you use the ICVERIFY SDK to produce receipt or report files, or if your own application code creates transaction requests containing cardholder data, you should securely delete this information as soon as you are finished using it. Consider the following:
 - Any transaction data stored on physical media should first be overwritten with meaningless characters, for example X’s or random characters, before being deleted. This will ensure that the physical media will not contain “ghost” data that could be recovered and abused by a hacker.
 - Application variables used to store sensitive data in application memory should be set to NULL or otherwise proactively deleted before being discarded. Don’t just wait for garbage-collection routines to handle the variables when they go out of scope.

If you use the shared-directory method:

- It is your responsibility to make sure the shared directory you use to interact with the ICVERIFY application is configured with the proper operating system permissions so that the .REQ and .ANS files can be properly read and deleted.
- If you produce receipts or reports using the SDK and use a “print-to-file” option rather than a physical printer, you need to ensure any report files generated are securely deleted after you have finished using them. The ICVERIFY application will *not* delete response files of any kind.
- ICVERIFY for Windows versions 4.0 and above offer you a 256-bit AES encryption library that you can use to process request and answer files in encrypted mode. If your integration is strongly bound to the shared-directory method, consider updating it to access the ICVERIFY encryption library for additional transaction security.
- Also, consider updating your integration to use the direct DLL interface (discussed in the *ICVERIFY SDK Guide*) to eliminate any risk of data remaining in the shared directory or in unused fragments on your hard drive. Bear in mind that the DLL offers both open-text and encrypted-mode interfaces as well; wherever possible, use the encrypted mode.

If you use the direct DLL interface:

- Aside from the file- and encryption-related comments above, you do not need to make any other adjustments to your software integration apart from a “secure deletion” review.

**Special Note
for Merchants
Using an
ICVERIFY
Enterprise
Edition SDK
Interface**

Merchants interacting with the ICVERIFY™ Enterprise Edition product through one of its SDK interfaces, including Java™, C++, ActiveX™ and native “Format 3” messages should bear the following in mind:

- **Secure Transmission of Data.** Some of the Enterprise SDK interfaces support encryption of the channel between your code and the Enterprise server (for example, the Secure Java API.) Consider using a secure-mode SDK for your transaction processing; consult the *ICVERIFY Enterprise Edition SDK Guide* for additional details. Note: If you are sending transactions over a wide-area or wireless network, you *must* encrypt your transactions, even if only a portion of the network connection consists of that type of link. You should also consider encryption at both the physical and application level.

Finally, as discussed earlier, certain security exposures have been identified with WEP Wireless Encryption Protocol. It is strongly recommended that you implement additional security measures over any WEP-based link, such as IPsec or SSL if you are not employing Wi-Fi Protected Access (WPA). Remember, any link over a public network, regardless of physical transport media used, should be secured by no weaker than 128-bit encryption.

- **Proper Use of a Currently Supported SDK.** It is your responsibility to ensure that you are using a currently supported SDK and that the payment transactions you process via that SDK are properly constructed. Each release of the ICVERIFY Enterprise product is tested to confirm sensitive data is properly handled when submitted by all currently supported SDK interfaces. However, interfaces originally published as part of a legacy application, such as ICVERIFY for MS-DOS™ and PCAuthorize™, are generally not tested. Therefore, unless you are using a currently supported SDK, we cannot make any assurances about the handling of sensitive data. Moreover, it is theoretically possible, though unlikely, that a malformed SDK message might have sensitive data logged by the server due to the data being in an incorrect location. We go to great lengths to cover all scenarios, no matter how unlikely, but can only assure you of the product's performance if you use a current SDK and construct your payment transactions properly.
- **Secure Deletion.** Please consult the notes about “Secure Deletion” earlier in this document. These guidelines may also apply to you.

**Special Note
for Merchants
Using an
ICVERIFY, Inc.
Product for
Internet
Payments**

Merchants using an ICVERIFY, Inc. software product to process payment transactions generated over the Internet, or merchants with an Internet line of business, should consider the following:

- **Segregate Web and Payment Systems.** Don't install and operate your payment software on the same system as your Web server. As stated earlier, if your payment software is installed on a computer that has direct access to the Internet, ensure that you have appropriate logical or physical firewalls in place to secure the computer. If you have written or purchased custom Web-facing software that also interacts with your ICVERIFY, Inc. product, segregate the Web-facing component on a separate computer from your payment software.
- **Practice Secure Web System Development.** Due to the nature of the Internet and the technologies used to enable browser-based communication with a Web site, there are specific requirements within the PCI standards to which you should adhere as you build your Web site. You should consult the Open Web Application Security Project at <http://www.owasp.org> for their recommendations on secure Web application development.
- **Other Guidelines.** Be sure to consult other sections of this document for important information that may apply to you, depending on the integration mode you have used to implement your ICVERIFY payment solution.

If You're Using Older Software

If you are using an ICVERIFY, Inc. product that was *not* tested to be in compliance with the data storage requirements, such as PCAuthorize™, ICVERIFY™ for MS-DOS™, or a version of ICVERIFY for Windows™ or WebAuthorize™ earlier than those listed in the most recent *Data Storage Statement*:

- **Upgrade Your Software.** We urge you to upgrade to a more recent version of software. The reasons are many, and include the following:
 - Software products older than the versions listed in the *Data Storage Statement* are **not** supported by ICVERIFY, Inc.
 - The product may not be in compliance with all applicable security requirements -- upgrading to one of the software releases listed at the beginning of this guide will ensure your software is in compliance with the standards in effect at the time this guide was produced.
 - Many changes to the credit card processing rules have occurred in the past few years, and you may be paying more than you should to process transactions to your bank.
 - Your acquiring bank or processing company may require that you upgrade to a PABP-certified software application.
 - Versions of software other than those explicitly listed in the *Data Storage Statement* will not be tested for PABP compliance.
 - You will not be able to take advantage of the many new features in the ICVERIFY product line with older software.

For these reasons, ICVERIFY, Inc. *strongly recommends* upgrading to the latest software. Call ICVERIFY Sales at (800) 538-0651 to learn more about our products and what an upgrade might offer you.

Additional Resources

Data and site security can be a complex effort. We hope this guide has been of value to you in your ongoing evaluation of your business and technical operations and the role of your ICVERIFY, Inc. product within them. Please remember, however, that ultimately it is your sole responsibility to conform to the applicable security regulations, guidelines and standards for your type of business and processing volume. ICVERIFY, Inc. can only provide general suggestions and guidance; the obligation to show and maintain compliance is yours. To assist you in your compliance efforts, we have compiled a list of important resources for your reference. These resources are by no means exhaustive and should be considered a starting point for your own investigation:

- **Visa Cardholder Information Security Program (CISP):** You can obtain the latest information about CISP at <http://www.visa.com/cisp>. Follow the appropriate links to determine your compliance obligations.
- **MasterCard Site Data Security (SDP):** You can obtain the latest information about SDP at <https://sdp.mastercardintl.com/>.
- **American Express Data Security Standards (DSS):** Review the latest high-level card security standards from American Express at http://www125.americanexpress.com/merchant/oam/ns/USEng/FrontServlet?request_type=navigate&page=generalRequirements.
- **Discover Card Information Security and Compliance (DISC):** You can obtain the latest information about the DISC program at http://www.discoverbiz.com/resources/data/data_security.html.
- **IMPORTANT NOTE!** Recently, the card associations have merged their various security programs into a unified standard called the Payment Card Industry (PCI) standard. You may be able to perform a single audit for the PCI standards instead of each individual program.

Some additional resources that may be applicable to you, depending on the type of merchant business you operate, are the following:

- **The Open Web Application Security Project (OWASP):** The free guides available at the OWASP site, <http://www.owasp.org>, are invaluable industry-standard resources, full of recommendations regarding installing and operating secure server-based applications.
- **Privacy Rights Clearinghouse:** A number of state laws regarding consumer privacy rights for credit card and check transactions can be found at <http://www.privacyrights.org/fs/fs15plus.htm>.