PADSS Implementation

01/04/2021 The Raiser's Edge 7.96.6403.x 4.0 PADSS Implementation US

The information in this manual has been carefully checked and is believed to be accurate. Blackbaud, Inc., assumes no responsibility for any inaccuracies, errors, or omissions in this manual. In no event will Blackbaud, Inc., be liable for direct, indirect, special, incidental, or consequential damages resulting from any defect or omission in this manual, even if advised of the possibility of damages.

In the interest of continuing product development, Blackbaud, Inc., reserves the right to make improvements in this manual and the products it describes at any time, without notice or obligation.

PADSS-2021

Contents

PCI DSS Implementation 1

Payment Card Industry and Payment Application Data Security Standards 1

Data Management 2

Sensitive Authentication Data and Cardholder Data Retention 2

Cardholder Data Encryption 4

Network Security 4

User Account Management 5

Firewall Management 5

Wireless Devices 6

Remote Access 6

Non-console Administrative Access 7

Internet-Accessible Systems 8

System Maintenance 8

PA DSS Implementation in Raiser's Edge 7.96.6403.x 9

Blackbaud Payment Service and Raiser's Edge 10

- When Cardholder Data is Entered into Raiser's Edge 10
- When Payments are Charged in Raiser's Edge 11
- Credit Card Updater Service Updates Cardholder Data 11

User Account Configuration and Security 12

Cardholder Data 12

Records 13

Batch 13

Import 13

Export 14

Merchant Accounts 14

Authentication Event Log 14

Electronic Funds Transfer 15

Auditing 15

File Access Auditing 16

Versioning Scheme 16

Rollback and Uninstall 17

Services and Protocols 17

Revision Information 17

PA DSS Implementation in Blackbaud NetCommunity 20
Blackbaud Payment Service and Blackbaud NetCommunity 20
User Account Security 21
Sensitive Authentication Data and Cardholder Data 21
Merchant Accounts 22
Website Design 22
Integration with The Raiser's Edge 22
Rollback and Uninstall 22
Services and Protocols 23
Secure Sockets Layer Configuration 23
Digital Certificates in Internet Information Server 23
Configure SSL in Blackbaud NetCommunity 23
SSL in Blackbaud NetCommunity 24
Configure SSL Settings in the Windows Registry 24
Additional SSL Information 25

PCI DSS Implementation

Payment Card Industry and Payment Application Data Security Standards 1
Data Management 2
Sensitive Authentication Data and Cardholder Data Retention 2
Cardholder Data Encryption 4
Network Security 4
User Account Management 5
Firewall Management 5
Wireless Devices 6
Remote Access 6
Non-console Administrative Access 7
Internet-Accessible Systems 8
System Maintenance 8

When you accept payment cards for donations or revenue, the security of the credit card information is very important. Used properly, Blackbaud programs can help you maintain this information in accordance with the Payment Card Industry Data Security Standard (PCI DSS). To help promote this awareness of the security requirements for credit card and cardholder data, this chapter provides information about PCI DSS and how it impacts your organization. With the proper security of credit card information, you can protect your constituents and clients from inconvenience and financial and personal loss, and help protect your organization from additional expense.

Note: This guide provides only an overview of PCI DSS requirements and recommended best practices to ensure compliance. For additional detail, visit https://www.pcisecuritystandards.org to download the PCI DSS specification.

Payment Card Industry and Payment Application Data Security Standards

Developed by Visa, the Payment Application Data Security Standard (PA DSS) requires software companies such as Blackbaud to develop secure programs that enable users to comply with the PCI DSS. To learn more about PA DSS and download the specification, visit https://www.pcisecuritystandards.org.

Note: The Payment Card Industry (PCI) Security Standards Council includes American Express, Discover Financial Services, JCB International, Mastercard Worldwide, and Visa Inc. and was formed to help implement consistent data security measures on a global basis.

Developed by the PCI Security Standards Council, the PCI DSS includes requirements for security management, policies, procedures, network architecture, software design, and other proactive measures. As an organization that collects payment card information, such as to process payments or donations, you must adhere to the PCI DSS and proactively protect this data. To learn more about PCI DSS and download the specification and its supporting documents, visit https://www.pcisecuritystandards.org.

Note: Depending on your organization and the number of payment card transactions you process, you may need to engage an external security assessment company to determine your level of compliance with PCI DSS and other security compliance programs. If you use an external assessor, we recommend you select one that is qualified and familiar with the latest requirements from the PCI Security Standards Council. To validate whether your organization is compliant with PCI DSS, we recommend you also visit https://www.pcisecuritystandards.org and complete the PCI Security Standards Council Self-Assessment Questionnaire.

Data Management

Encryption is necessary to protect cardholder data. If a user circumvents security controls and gains access to encrypted data, without the proper cryptographic keys, the user cannot read or use the data. To reduce the risk of malicious abuse, you must consider other effective methods to protect stored data. For example, store cardholder data only when it is absolutely necessary, and do not send the cardholder data in unencrypted email messages.

Sensitive Authentication Data and Cardholder Data Retention

You should keep the storage of cardholder data to a minimum. To comply with PCI DSS, your organization must develop and maintain a data retention and disposal policy.

Raiser's Edge does not store, log, or display cardholder data or Primary Account Numbers (PANs). Users can enter PANs, but numbers are masked as soon as users tab out of the field, and only masked PANs are displayed after the initial entry on all displays, including point-of-sale devices, screens, logs, and receipts.[1] The program only stores and displays truncated cardholder data (last 4 digits). We cannot provide or retrieve cardholder data under any circumstances, even for troubleshooting or debugging purposes.[2]

The application cannot be configured such that only personnel with a legitimate business need can see unmasked PANs.[3]

- Limit the cardholder data stored and the retention time to only that which is required for business, legal, and regulatory purposes.
- Securely delete cardholder data once it is no longer required for these purposes.
- Securely delete cardholder data that exceeds your defined retention period.

[1] This practice complies with PA-DSS requirement 2.2.a.

[2] These practices comply with PA-DSS requirements 2.1, 2.2, 2.3, 2.4, 2.5, 2.5.1-2.5.7, and 2.6.

[3] This complies with PA-DSS requirement 2.2.a and 2.2.c.

While PANs may be displayed in the application, they are never stored. The table below details where data is stored or viewed and how it is encrypted and secured.

Data Store (file, table, etc.)	Cardholder Data Elements stored (PAN, expiry, any elements of SAD)	How data store is secured (for example, encryption, access, controls, truncation, etc.)	How is access to data store logged (logging mechanism)
GIFT Table	Truncated card number, expiry, cardholder name, card token	Truncated to last 4 digits	Access to the application is logged in an audit table.
CONSTITUENT+CREDITCARDS Table	Truncated card number, expiry, cardholder name, card token	Truncated to last 4 digits	Access to the application is logged in an audit table.
BATCHGIFT Table	Truncated card number, expiry, cardholder name, card token	Truncated to last 4 digits	Access to the application is logged in an audit table.
BATCHCONSTITDATA Table	Truncated card number, expiry, cardholder name, card token	Truncated to last 4 digits	Access to the application is logged in an audit table.
Profile Reports (Constituent, Individual, and Organization)	Truncated card number, expiry, cardholder name	Display truncated last 4 digits	Access to the application is logged in an audit table.
Batch Reports (batch credit card, credit card exception, credit card updater, gift entry validation, and batch deposit ticket reports)	Truncated card number, expiry, cardholder name	Display truncated last 4 digits	Access to the application is logged in an audit table.

Do not retain sensitive authentication data, such as the full magnetic stripe, card validation code, or personal identification number (PIN) information, in your database. The application does not collect cardholder data for troubleshooting purposes. If you must retain sensitive authentication data, such as for troubleshooting purposes, you must follow these guidelines: [1]

- Collect sensitive authentication data only when necessary to solve a specific problem.
- Store sensitive authentication data only in specific, known locations with limited access.
- Collect only the limited amount of data necessary to solve a specific problem.
- Encrypt sensitive authentication data while stored.
- Securely delete sensitive authentication data after use.

[1] These guidelines comply with PA-DSS requirement 1.1.5.

Warning: To comply with PCI DSS, you must remove historical sensitive authentication data and cardholder data from your database. If you upgrade from a non-compliant version, or if your organization used attributes, notes, or text-free fields to store sensitive authentication information or cardholder data, you must search for and securely delete this data from your database to comply with PCI DSS. This data includes track data, card verification codes, PINs, and PIN blocks. [1]

To ensure the complete and secure removal of cardholder data, you must securely erase temporary files that may contain sensitive authentication information and cardholder data.

- If you use Microsoft *Windows XP* or *Windows Vista*, turn off System Restore on the System Properties screen. To track changes in *Windows*, System Restore creates and uses restore points, which may retain cardholder data. When you turn off System Restore, the operating system automatically removes existing restore points and stops the creation of new restore points.
- To ensure the complete removal of data, install and run a secure delete tool such as Heidi *Eraser*. With a secure delete tool, you can safely erase temporary files that may contain sensitive information or cardholder data. For information about how to install and run the secure delete tool, refer to the manufacturer's documentation.

Cardholder Data Encryption

To comply with PCI DSS, your organization must encrypt cardholder information during transmission over open public networks that malicious users could abuse to intercept, modify, and divert data during transit. These open public networks include the Internet, WiFi (IEEE 802.11x), the global system for mobile communication (GSM), and general packet radio service (GPRS). To safeguard sensitive authentication information and cardholder data during transmission, use strong cryptography and security protocols such as Transport Layer Security (TLS) version 1.2 (or above) and Internet Protocol Security (IPSEC).

Raiser's Edge uses TLS 1.2 AES 256 encryption and does not transmit unencrypted cardholder data. For security purposes, ***Raiser's Edge*** does not allow fallback to SSL. Always verify that only trusted keys and/or certificates are accepted. [2]

Never send unencrypted cardholder data using end-user messaging technology.[3]

Network Security

With a secure network, you can protect your system and credit card information from internal and external malicious users. To secure your network, we recommend you utilize a firewall and configure wireless devices and remote access software.

[1] These guidelines comply with PA-DSS requirements 1.1.4 and 3.2.

[2] These guidelines comply with PA-DSS requirement 11.1.

[3] This guideline complies with PA-DSS requirement 11.2.a.

User Account Management

To comply with PCI DSS, you must assign unique identification to each person who accesses networks, workstations, or servers that contain the program or cardholder data. Unique login credentials ensure that only authorized users can access and work with the critical data and systems included in your network. With unique login credentials, you can also trace actions on your network to specific users. These credentials must include a unique user name and a way to authenticate the user's identity, such as a complex password, a token key, or biometrics. Because the application does not store Primary Account Numbers (PANs), even users with full administrative access cannot see this information. Only truncated account data (last 4 digits) is displayed in the application.[1]

At a minimum, your organization must implement these guidelines to create network user accounts and manage user authentication and passwords. You must communicate password procedures and policies to all users who can access cardholder data.

- Use authorization forms to control the addition, deletion, and modification of user IDs.
- Verify the identity of users before you reset passwords.
- Immediately revoke account access for terminated users.
- Remove or disable inactive user accounts at least every 90 days.
- Enable user accounts for use by vendors for remote maintenance only when needed, and immediately deactivate them after use.
- Do not use group, shared, or generic user accounts and passwords.
- Require users to change their initial passwords immediately after the first use and subsequent passwords at least every 90 days.
- Require passwords with a minimum length of seven numeric and alphabetic characters.
- Require that new passwords not match one of the last four passwords used by the user.
- Lock out the user account after no more than six failed login attempts. Set the lockout duration to 30 minutes or until a system administrator enables the user account.
- Log out idle sessions after 15 minutes so users must enter the password to activate the workstation.
- To log user authentication and requests, turn on database logging in Microsoft *SQL Server*.

Firewall Management

If you use software to process payments, we recommend you verify that the workstation's link to the Internet is secure. If you transfer transactions online, ensure your Internet hardware, such as the modem or DSL router, provides a built-in firewall. You must restrict connections between publicly accessible servers and any system component that stores cardholder data, including connections from wireless networks. The Blackbaud application does not store cardholder data, and only truncated card data is displayed (last 4 digits).[2]

[1] These guidelines comply with PA-DSS requirement 3.1.

[2] This complies with PA-DSS requirement 9.1.

Wireless Devices

Blackbaud does not provide a wireless payment application. If you choose to use the application in a wireless setting, follow these guidelines to be in compliance.[1]

- Install perimeter firewalls between any wireless networks and systems that store cardholder data. These firewalls must deny or control any traffic necessary for business purposes from the wireless environment to the cardholder data environment.
- Implement strong encryption, such as Advanced Encryption Standard (AES), on all wireless networks.
- At installation, change wireless encryption keys, passwords, and SNMP community strings from the default. After installation, change wireless encryption keys, passwords, and SNMP community strings when anyone with knowledge of these items leaves the organization or changes positions with the organization.
- Do not use the vendor-supplied defaults for the wireless environment. Change the default passwords or pass phrases on access points and single network management protocol (SNMP) community strings on wireless devices.
- Change the default service set identifier (SSID) and disable SSID broadcasts when applicable.
- Update the firmware on wireless devices to support strong encryption—such as WiFi-protected access (WPA or WPA2) technology, Internet Protocol security virtual private network (IPSec VPN), or Transport Layer Security (TLS)—for authentication and transmission over wireless networks.
- Use industry best practices (for example, IEEE 802.11i) to implement strong encryption for the transmission of cardholder data and sensitive authentication data over the wireless network in the cardholder data environment.

To comply with PCI DSS, your organization must configure all mobile and employee-owned computers with direct connectivity to the Internet, such as laptop computers, used to access the network with an installation of personal firewall software. The firewalls must be active and configured to a specific standard that users cannot alter.

Remote Access

The Blackbaud payment functionality is accessible only to users with access to your organization's network. The application is configured to only be accessible with network access by default. Blackbaud does not have nor require access to customer networks in order to install the payment application. Updates are not delivered via remote access from Blackbaud.

If your organization allows for remote network access by employees, administration, and vendors, you must implement multi-factor authentication for logins in order to meet PCI-DSS requirements. Multi-factor authentication requires unique login credentials (username and password) and additional authentication items such as a token or individual certificate. Use of technology such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens or VPN (based on TLS or IPSec) with individual certificates are acceptable methods of multi-factor authentication.

[1] These guidelines comply with PA-DSS requirements 6.1 and 6.3.

To comply with PCI DSS, your organization must configure the remote access software to ensure network security. [1]

- Do not use the vendor-supplied defaults, such as passwords, for the remote access software.
- Establish unique login credentials and complex passwords for remote access users in accordance with PCI DSS requirements 8.1.5 and 8.3. For information, see User Account Management on page 5.
- Allow connections from only specific known IP and MAC addresses.
- Enable encrypted data transmission in accordance with PCI DSS 4.1.
- Lock out the remote access user account after no more than six failed login attempts.
- Require remote access users to establish a VPN connection through a firewall before they connect to the network.
- Enable the logging function.
- Establish complex passwords for customers in accordance with PCI DSS requirements 8.2.3.
- Restrict access to customer passwords to authorized third-party personnel.
- To verify the identities of remote access users, require multi-factor authentication such as both a user login and a password.

If your organization enables remote access for use by vendors, it should be only when needed and immediately deactivated after use.

Non-console Administrative Access

To comply with PCI DSS, your organization must encrypt all non-console administrative access. For web-based management and other non-console administrative access, use technologies such as Secure Shell (SSH), VPN, or TLS.

You must use multi-factor authentication in order to comply with PCI DSS requirements.

If you use Remote Desktop (RDP) for non-console administrative access, it is advised that you follow best practices for RDP security such as digitally signing RDP files with a custom certificate, tightening connection security through a TLS security layer and raising the encryption level to high, and using network level authentication. You should use multi-factor authentication for all personnel with non-console administrative access.

Raiser's Edge does not provide a non-console administrative access solution. [2]

For information on configuring RDP security, see Microsoft documentation at https://technet.microsoft.com/en-us/library/cc753488.aspx.

[1] These guidelines comply with PA-DSS requirements 10.1, 10.2, 10.2.1, and 10.2.3.

[2] These guidelines comply with PA-DSS requirements 12.1, 12.1.1, and 12.2.

Internet-Accessible Systems

Do not store cardholder data on Internet-accessible systems. For example, do not house the database server within the same server as the web server.

System Maintenance

Once you secure your system, you must keep your software and equipment current. Malicious users can use security vulnerabilities to access your system. Both hardware and software manufacturers occasionally issue updates to products, such as to remedy these vulnerabilities and help prevent such attacks. We recommend you ensure you have the most recently released patches installed. For example, you can frequently review the manufacturer's websites, newsletters, and online forums to check for the current patches.

Blackbaud frequently releases patches and updates for all our applications. You are responsible for keeping your Blackbaud software up to date. Releases and patches are available for secure download on the Blackbaud website behind your customer password. You are notified of releases and patches as they are available through email communication. [1] Blackbaud does not deliver updates to you remotely, sends you a direct download link, or sends a physical CD or DVD with an install or update; the only way to download an update is to securely log into the Blackbaud website with your customer credentials.[2] All packages are digitally signed to ensure integrity.

Occasionally, a manufacturer may stop support of a product. In this case, we recommend you determine whether your organization should continue to use an unsupported product. Also, a manufacturer may inform you of a flaw or defect in a product that may make your organization vulnerable to attack. We recommend you pay attention to these alerts and update your system accordingly.

To further reduce vulnerability, we recommend you also deploy anti-virus software on your systems and ensure they are current, actively running, and can generate assessment logs.

[1] These guidelines comply with PA-DSS requirement 7.2.3.

[2] This complies with PA-DSS requirement 10.2.1.

PA DSS Implementation in Raiser's Edge 7.96.6403.x

Blackbaud Payment Service and Raiser's Edge 10
User Account Configuration and Security 12
Cardholder Data 12
Records 13
Batch 13
Import 13
Export 14
Merchant Accounts 14
Authentication Event Log 14
Electronic Funds Transfer 15
Auditing 15
File Access Auditing 16
Versioning Scheme 16
Rollback and Uninstall 17
Services and Protocols 17
Revision Information 17

Raiser's Edge 7.96.6403.x includes features to help you secure your data and comply with PCI DSS. We strongly recommend you update your software to version 7.96.6403.x[1] There are no other application dependencies required in order to configure ***Raiser's Edge*** in compliance with PCI DSS.[2]

This guide is available and disseminated to all customers, resellers, and integrators for ***Raiser's Edge***. The guide is available on the Blackbaud website, and can be provided to any customer, reseller, or integrator upon request.[3] This guide is updated at least once annually.

It is also updated when there are changes made to ***Raiser's Edge*** and when PA-DSS requirements change.[4]

[1] This guideline complies with PA-DSS requirement 13.1.1.

[2] This guideline complies with PA-DSS requirement 13.1.1.

[3] This complies with PA-DSS requirement 13.1.

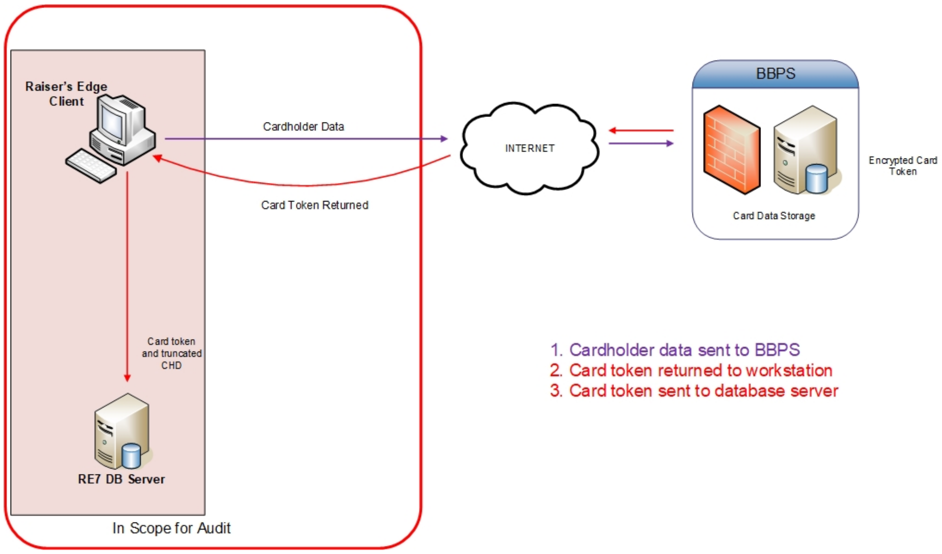
[4] This complies with PA-DSS requirement 13.1.3.a.

When the implementation guide is updated, the revision information is updated and the last updated date is changed on the guide and on the website. This allows customers, resellers, and integrators to access the latest version.[1]

Blackbaud Payment Service and Raiser's Edge

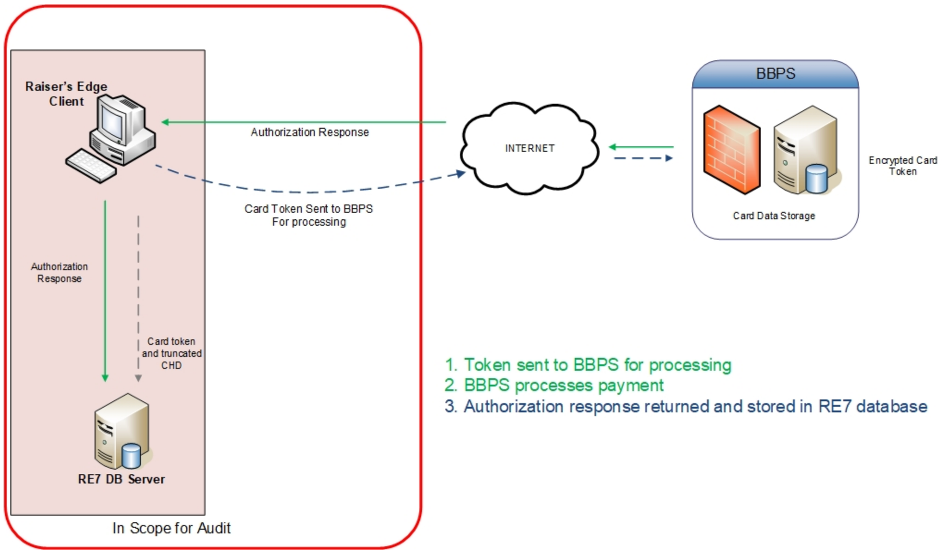
Raiser's Edge 7.96.6403.x does not store complete credit card numbers in the database. To store credit card and merchant account information, the program uses the ***Blackbaud Payment Service***. When you first update **Raiser's Edge**, you select whether to send your existing credit card information to the web service or simply mask the credit card numbers in your database. If you process recurring credit card payments through ***Raiser's Edge***, the program uses the ***Blackbaud Payment Service*** to transmit credit card information and process transactions through your merchant accounts.

When Cardholder Data is Entered into Raiser's Edge



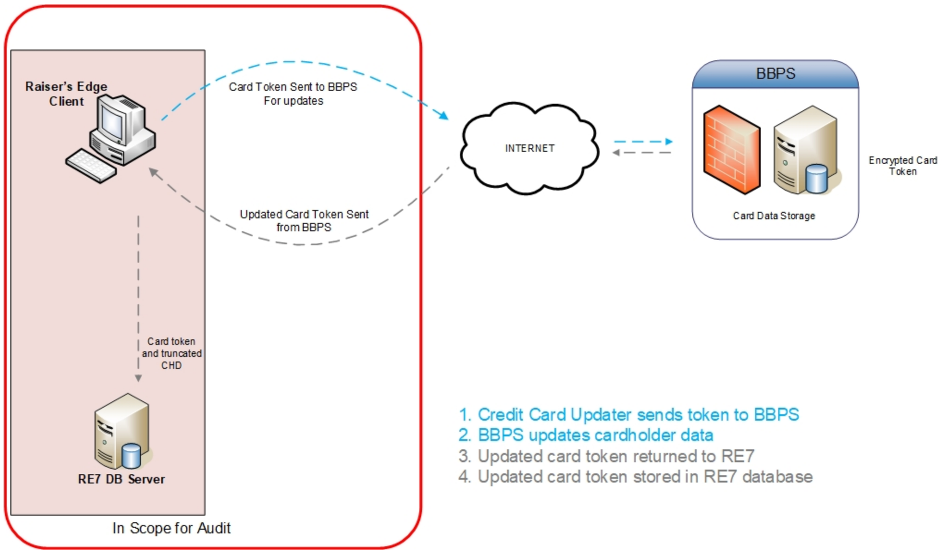
[1] This complies with PA-DSS requirement 13.1.3.c.

When Payments are Charged in Raiser's Edge



1. Token sent to BBPS for processing
2. BBPS processes payment
3. Authorization response returned and stored in RE7 database

Credit Card Updater Service Updates Cardholder Data



1. Credit Card Updater sends token to BBPS
2. BBPS updates cardholder data
3. Updated card token returned to RE7
4. Updated card token stored in RE7 database

Note: Raiser's Edge does not send incomplete credit card numbers, or those associated with one-time gifts such as donations, to the ***Blackbaud Payment Service***. During the update process, ***Raiser's Edge*** removes these credit card number from your database and retains only the last four digits.

When you first submit credit card information to the ***Blackbaud Payment Service*** for storage, it create a unique reference number for each credit card number to securely identify and process transactions in accordance with PCI DSS.

User Account Configuration and Security

Raiser's Edge requires the use of strong or complex passwords.

- Passwords are case-sensitive and require numeric and alphabetic characters.
- Passwords can have up to 50 characters but must have a minimum of eight
- In *Configuration*, you can confirm business rules to require users to change their passwords on a routine basis. New passwords entered by users cannot match one of the last four passwords used by the user.

Warning: To help secure user login credentials, you must use *Windows* authentication with ***Raiser's Edge***. *Windows* authentication uses security support providers (SSPs), installed as dynamic-link libraries (DLLs), as protocols to verify the credentials of users and control the connection, communication, and data transfer between computers in a *Windows* environment. For information about *Windows* authentication, see http://technet.microsoft.com/en-us/library/cc755284.aspx.

To secure your database, ***Raiser's Edge*** automatically locks out a user account after a specified number of failed login attempts. To prevent further attempts, a locked user account remains locked for a specified time period. In *Configuration*, you can configure business rules to specify the number of failed attempts to allow before the program locks the user account and the duration of the lockout.

Warning: To comply with PCI DSS, you must require users to change passwords at least every 90 days and lock out a user account after no more than six failed login attempts. You must set the lockout duration to 30 minutes or until a system administrator enables the user account. For information about additional password and lockout requirements for PCI DSS, see User Account Management on page 5.

For additional security, ***Raiser's Edge*** automatically logs out a user when the session is idle for 15 minutes. To activate the workstation, the user must enter the password again.

Cardholder Data

Raiser's Edge 7.96.6403.x automatically removes all credit card numbers from these records in your database when revisions run the first time you log in:

- Bio 2 or Org 2 tab on a constituent record
- Gift record with credit card information
- Constituent or gift batch that contains credit card information
- United Way *Workplace Giving* pledge envelope record that contains credit card information

When you enter new credit card information into the program, it automatically sends the data to the ***Blackbaud Payment Service*** for storage and retains the reference number generated by the web service. For reference, only the last four digits of credit card numbers appear in the program.

Your organization can use attributes, notes, and free-text fields to store important information. However, do not use these features to store sensitive information, such as payment card or cardholder data, in the program. The abuse or misuse of the program to store sensitive information can leave you vulnerable to an attack by malicious users. For information about the data management requirements of PCI DSS, see Data Management on page 2.

Warning: If your organization used attributes, notes, or free-text fields to store sensitive cardholder information, you must delete these attributes and information from your database. For information about how to delete attributes from ***Raiser's Edge***, see the *Configuration and Security Guide*.

Raiser's Edge does not facilitate the transmission of primary account numbers (PANs) through messaging technology such as email or instant messages. [1]

Records

When you create a new constituent or gift record, the program automatically sends the credit card information entered to the ***Blackbaud Payment Service*** when you click **Save and Close**. On the saved record, only the last four digits of the credit card number appear.

In accordance with PCI DSS, your organization must develop and maintain a data retention and disposal policy. You must keep cardholder data storage to a minimum and limit the retention time to only the duration required for business, legal, and regulatory purposes. In *Administration*, you can use **Globally Change Records** to easily remove data such as cardholder name, credit card number, and expiration date from selected records in your database in ***Raiser's Edge*** in accordance with your data retention and disposal policy. For information about **Globally Change Records**, see the *Global Add, Delete, and Change Guide*.

Batch

When you enter credit card information in a batch, the program sends this data to the ***Blackbaud Payment Service*** when you leave the row in the data entry grid and displays only the last four digits of the entered credit card number.

While ***Raiser's Edge*** removes credit card numbers from existing constituent and gift batches and prevents the committal of credit card numbers to records through *Batch*, temporary files may exist of batches generated with a previous version that contain sensitive cardholder information. To comply with PCI DSS, you must use a real deletion tool to permanently remove temporary files that contain sensitive credit card information.

Tip: Temporary batch files generated by ***Raiser's Edge*** have names that begin with "BB67". The batch files that contain credit card information have an extension of *.mdb. To search for temporary batch files to delete, we recommend you use the search criteria of "BB67*.mdb".

If you use *Batch* to authorize credit card transactions, ***Raiser's Edge*** does not generate the transmission files used to process these transactions. Instead, the program sends this data to the ***Blackbaud Payment Service***, which uses your merchant accounts to process the payments through the selected gateways.

Import

When you import credit card information into ***Raiser's Edge***, the program automatically sends this data to the ***Blackbaud Payment Service***. In the import file generated, only the last four digits of the

[1] These details comply with PA-DSS requirement 11.2.

credit card numbers appear.

> ***Note:*** The credit card information you import into ***Raiser's Edge*** must be valid and complete. You cannot import masked credit card numbers into the database. Invalid or incomplete credit card information causes an exception during the import.

Export

In accordance with PCI DSS, you cannot export sensitive cardholder data from ***Raiser's Edge 7.9*** or later. Exported credit card numbers appear as a series of asterisks followed by the last four digits of the credit card number.

Merchant Accounts

Raiser's Edge 7.96.6403.x does not store unencrypted login credentials for merchant accounts in the database. The program uses the ***Blackbaud Payment Service*** to store your organization's merchant account information.

Raiser's Edge can retrieve your merchant account information from the ***Blackbaud Payment Service***, with the exception of the login and password required to connect to the merchant account. If your organization uses additional Blackbaud programs that process payments, such as ***Blackbaud NetCommunity***, you can now view and select merchant accounts added through that program in ***Raiser's Edge***.

Authentication Event Log

To help your organization track users who access the database, ***Raiser's Edge*** maintains an authentication event log. When a user logs into ***Raiser's Edge***, the program automatically records the event, including the name of the user, the network name of the machine used, the times the user logs in and out, and whether the user connects to the database through ***Raiser's Edge*** or another venue such as an integrated installation of ***Blackbaud NetCommunity***.

To check user login activity, you can access the authentication event log through the database.

- For a *SQL Server* database, use the script SELECT * FROM dbo.LOGINAUDIT.
- For an *Oracle* database, use the script SELECT * FROM rewin.LOGINAUDIT.

After you complete your query in Microsoft *SQL Server Management Studio*, you can save the log locally or on your network as a comma-separated value (*.csv) file. On the Results tab, right-click in the grid, select **Save Results As**, select CSV as the file type, specify the name and location to save the file, and click **Save**. You can then import the saved file into your centralized logging system.

To automate this process, you can set up a Windows scheduler to run a statement following this pattern: SQLCMD -S <SERVERNAME> -d <DATABASENAME> -E -Q "select LOGINCONNECTIONID, MACHINENAME, USER_ID, USER_NAME, MODULENUM, DESCRIPTION, LOGIN_TIME, LOGOUT_TIME from dbo.LOGINAUDIT" -s "," -o "D:\MyLogData.csv". [1]

[1] These guidelines comply with PA-DSS requirement 4.4.

Electronic Funds Transfer

If your organization selects to use the ***Blackbaud Payment Service*** to store credit card information, you can use the optional module *Electronic Funds Transfer* to process credit card payments. ***Raiser's Edge*** does not include unencrypted credit card numbers in the transmission files generated by the credit card process. Instead, the transmission files include the reference number received from the ***Blackbaud Payment Service*** for each credit card number. To process credit card transactions, ***Raiser's Edge*** sends the transmission file to the ***Blackbaud Payment Service***, which replaces the reference numbers with their corresponding credit card numbers and then sends the transmission file to your payment gateway for authorization. For information about the ***Blackbaud Payment Service***, see Blackbaud Payment Service and Raiser's Edge on page 10.

While ***Raiser's Edge 7.96.6403.x*** prevents access to the transmission files generated to process credit card transactions, previous versions of the program allowed access to copies of the files to debug or retain for history. When you generated copies of these transmission files, ***Raiser's Edge*** may have created temporary files of the copies. Since these transmission files contain sensitive credit card information, your organization must securely manage these files in accordance with PCI DSS. To comply with PCI DSS, you must use a real deletion tool to permanently remove temporary files that contain sensitive credit card information. To delete temporary transmission files, search for and delete files with an *.ans or *.req extension.

Auditing

Once you secure your system, you must monitor and track access to the network and your credit card information, such as with logging mechanisms. The lack of activity logs can make the determination of the cause of an attack very difficult. Logs help you track and analyze network activity when something goes wrong. To further reduce vulnerability, we recommend you also frequently test your network to verify its security continues to be maintained, regardless of age or changes in software.

Raiser's Edge does not store cardholder data or provide access to cardholder data.

To comply with PCI DSS, you must implement automated audit trails for all system components to track these events: [1]

- All individual users who access cardholder data.
- All actions performed by users with root or administrative privileges.
- All access of the audit trails.
- All invalid logical access attempts.
- All use of identification and authentication mechanisms.
- The initialization of the audit logs.
- The creation and deletion of system-level objects.

For each event, your organization must also record these audit trail entries for all system components:

[1] These guidelines comply with PA-DSS requirement 4.1.

- The user who initiates the event.
- The type of event.
- The date and time of the event.
- Whether the event succeeds or fails.
- The origination of the event.
- The data, system component, or resource the event affects.

File Access Auditing

In order to comply with PA-DSS requirements, you must log file access for the ***Raiser's Edge*** . Blackbaud provides a utility to turn on Windows file audit policies for the Raiser's Edge installation folder, which will log all file access to the Windows Event Viewer. This utility also disables weak TLS ciphers.[1] You must run this utility to be in compliance with PA-DSS. You only need to run this utility once.

To run this utility, follow these steps.

1. Go to www.blackbaud.com. From the **Support** menu, select **Downloads**.
2. Log in to access your downloads.
3. Select the **The Raiser's Edge 7 PA-DSS Utility**.
4. On the screen that appears, select the zip file to download it.
5. Extract the zip file.
6. In the folder where the files are unzipped, right-click the .exe file and select **Run as administrator**.
7. The **Install Location** field defaults to where the ***Raiser's Edge*** install files are most commonly located. Make sure this location is correct for your setup, and make any necessary changes to the file path.
8. Select **Run utility**. Once the utility runs successfully, you will see a confirmation message on the screen.

Versioning Scheme

Raiser's Edge follows a numeric versioning scheme to identify the latest software release and the type of update. The versioning scheme structure is the major release number, minor release number, build number, and patch, each separated by a period:[2]

major.minor.build.patch

The major release number increases when significant changes to the product’s architecture are made. The minor release number increases when broad changes to the product’s functionality or user

[1] This complies with PA-DSS requirements 4.2.7, 11.1.a, and 11.1.c.

[2] These details comply with PA-DSS requirement 5.4.4.

interface are added. A build number change indicates behavior or user interface, such as adding, removing, or changing specific behavior, are made and could indicate a security-impacting change to the system. The patch segment is a wildcard character and will be incremented with each patch to a build. The patch segment indicates smaller product changes and could include cosmetic changes or minor functionality changes and will never indicate a security-impacting change. The build segment is the only segment which, when changed, could imply a security-impacting change. When a security-impacting change is made, the Release Notes for that version will communicate the security impact. When no security-impacting change is made, the Release Notes will indicate as such.

Rollback and Uninstall

Before you install any updates, we strongly recommend you back up your database. For information about the update process, see the *Update and New Features Guide*.

If you encounter problems during the installation process, you can cancel the installation before it finishes. After you cancel, the install utility returns your machine to its state before the installation. If you complete the installation process but feel the program may have installed improperly, you can sue the **Add or Remove Programs** utility, available from the Control Panel in *Windows*-based operating systems, to safely uninstall the application.

All installation and update guides are available from the user guides area of our website at https://www.blackbaud.com/training-support/support/howto/raisers-edge#guides.

Services and Protocols

Raiser's Edge does not require the use of any insecure services or protocols. The services and protocols that ***Raiser's Edge*** requires are Transport Layer Security (TLS) 1.2 and Hypertext Transfer Protocol Secure (HTTPS). All required protocols, services, components, and dependent software necessary are included in the ***Raiser's Edge*** install. [1]

Revision Information

This guide is reviewed and updated as necessary on a yearly basis and based on changes to ***Raiser's Edge*** or the PCI DSS and PA DSS specifications.[2] Blackbaud distributes this guide through the user guides page on our website at https://www.blackbaud.com/training-support/support/howto/raisers-edge#guides.

Author	Revision date	Summary of changes
Steve Stegelin (Technical Writer III)	March 2009	Created guide.

[1] These details comply with PA-DSS requirement 8.2.

[2] This complies with PA-DSS requirement 13.1.3.

Author	Revision date	Summary of changes
Steve Stegelin (Senior Technical Writer)	June 2010	Reviewed guide. No updates made.
Steve Stegelin (Senior Technical Writer)	January 2011	Updated document template.
Steve Stegelin (Senior Technical Writer)	March 2012	Updated WEP warning to include WPA2 recommendation; Updated references to SSL and TLS with version number; Replaced references to "primary account number (PAN)" with "cardholder data"; Removed references to ICVerify; Updated Authentication Event Log on page 14; Added this table and Services and Protocols on page 17.
Steve Stegelin (Information Architect)	June 2012	Updated document template; minor edit to remove recent-speaking terms such as "now" and "new".
Steve Stegelin (Information Architect)	June 2013	Reviewed guide. No updates made.
Steve Stegelin (Information Architect)	July 2014	Updated version number to include ***7.93***.
Britt Murray (Staff Technical Writer)	December 2015	Updated version number to include ***7.95***. Removed duplicate word, Guide, from title page.
Lindsey Rix (Senior Staff Technical Writer)	October 2016	Updated version number to include ***7.96***.
Paula Koetter (Staff Technical Writer)	May 2017	Removed references to NetSolutions. Changed product name to ***Raiser's Edge*** instead of ***The Raiser's Edge***. Removed references to SSL; replaced with TLS. Removed references to ***Raiser's Edge 7.6***. Added footnotes to identify compliance with specific PA-DSS requirements. Added details about what type of historical cardholder data must be removed from the database. Added note about components included in the ***Raiser's Edge*** install.
Paula Koetter (Staff Technical Writer)	July 2017	Updated to indicate that we require the use of Windows Authentication. Previously, this was encouraged but not required.

Author	Revision date	Summary of changes
Paula Koetter (Staff Technical Writer)	August 2017	Updated with footnotes to indicate compliance with specific PA-DSS requirements. Added note to indicate that the payment application does not collect cardholder data for troubleshooting purposes. Added note to indicate that users cannot access more than masked PANs. Added details about how updates are delivered to clients. Removed references to ***Blackbaud CRM***.
Paula Koetter (Staff Technical Writer)	October 2017	Added recommendation to use multi-factor authentication. Updated versioning scheme to reflect major.minor.build.patch numbering format. Added information for automating the log file tracking.
Paula Koetter (Staff Technical Writer)	January 2018	Changes to Versioning section. Updated version number for ***Raiser's Edge*** to 7.96.01.x. Removed references to PA-DSS requirements 6.1 and 6.2. Removed recommendations for how to safely store cardholder data since the Blackbaud application does not store cardholder data. Clarified that Blackbaud does not deliver software updates remotely. Clarified that ***Raiser's Edge*** does not transmit unencrypted cardholder data. Added information about multi-factor authentication for personnel with non-console administrative access.
Paula Koetter (Staff Technical Writer)	March 2018	Added File Access Auditing section. Edited Wireless Devices section to clarify that Blackbaud does not provide a wireless application and we do not recommend that they use the payment application wirelessly. Added information about places where PANs might be displayed. Updated ***Raiser's Edge*** version number. Included information about how upgrades are delivered and indicated that they are digitally signed. Clarified application dependencies for compliance. Added information about how this guide is disseminated and updated.
Paula Koetter (Staff Technical Writer)	April 2018	Updated version number for ***Raiser's Edge*** to 7.96.6402.x.
Paula Koetter (Staff Technical Writer)	May 2018	Added more explicit language on requirements 2.2.a and 2.2.c, indicating that no users can get access to see unmasked PANs and that no unmasked PANs are displayed on any screen. Clarified that credit card numbers are truncated to the last 4 digits. Added table listing each location where cardholder data is stored and how it is encrypted or secured and logged.
Paula Koetter (Principal Technical Writer)	September 2019	Streamlined diagram of cardholder data workflow.
Paula Koetter (Principal Technical Writer)	December 2020	Updated version number for ***Raiser's Edge*** to 7.96.6403.x. Updated old URL links.

PA DSS Implementation in Blackbaud NetCommunity

Blackbaud Payment Service and Blackbaud NetCommunity 20
User Account Security 21
Sensitive Authentication Data and Cardholder Data 21
Merchant Accounts 22
Website Design 22
Integration with The Raiser's Edge 22
Rollback and Uninstall 22
Services and Protocols 23
Secure Sockets Layer Configuration 23
Digital Certificates in Internet Information Server 23
Configure SSL in Blackbaud NetCommunity 23
SSL in Blackbaud NetCommunity 24
Configure SSL Settings in the Windows Registry 24
Additional SSL Information 25

Blackbaud NetCommunity 6 or later, including the current ***6.64***, provides enhancements to help you secure your data and comply with PCI DSS. We strongly recommend you update your software to this version.

Blackbaud Payment Service and Blackbaud NetCommunity

Blackbaud NetCommunity does not store complete credit card numbers in its database. To securely store credit card and merchant account information, ***Blackbaud NetCommunity*** uses the ***Blackbaud Payment Service***. When you update to ***Blackbaud NetCommunity 6*** or later, the program automatically sends your existing credit card information to the web service. If you process credit card payments through ***Blackbaud NetCommunity***, the program uses the ***Blackbaud Payment Service*** to transmit credit card information and process transactions through your merchant accounts. When you first submit credit card information to the ***Blackbaud Payment Service*** for storage, it creates a unique reference number for each credit card number to securely identify and process transactions in accordance with PCI DSS.

In *Administration*, you can manage your login credentials for the ***Blackbaud Payment Service*** from the Configuration page. ***Blackbaud NetCommunity*** uses this information to communicate with the web service.

User Account Security

To comply with PCI DSS, you must change the supervisor login credentials from the default to a unique login name and complex password. We recommend you also change the login credentials of all default user accounts from their default settings and disable any user accounts your organization does not use. In *Administration*, you can edit the login credentials and manage user accounts as necessary.

In *Administration*, you can select to require users to use complex passwords from the System Options page. Complex passwords require at least eight characters, including one upper-case and one lower-case letter and either a special character or number. If you do not select **Require complex passwords**, you must configure the minimum number of characters required and select whether passwords are case-sensitive.

To secure your database, ***Blackbaud NetCommunity*** can automatically lock out a user account after a specified number of failed login attempts. To prevent further attempts, a locked user account remains locked for a specified time period. On the System Options page, you can configure business rules to specify the number of failed attempts to allow before the program locks the user account and the duration of the lockout.

Warning: Do not change the default installation settings for the requirement of unique user login credentials and secure authentication. Adjustment from the default settings and requirements will result in noncompliance with PCI DSS.

For information about additional password and lockout requirements for PCI DSS, see User Account Management on page 5.

Sensitive Authentication Data and Cardholder Data

When you enter new credit card information into ***Blackbaud NetCommunity 6*** or later, the program automatically sends the data to the ***Blackbaud Payment Service*** for storage and retains the reference number generated by the web service. For reference, only the last four digits of the credit card numbers appear in the program.

Note: Prior to version 6, ***Blackbaud NetCommunity*** stored unencrypted cardholder data. After you update to ***Blackbaud NetCommunity 6*** or later, the program securely deletes cardholder data and sends it to the ***Blackbaud Payment Service*** for storage. Since ***Blackbaud NetCommunity 6*** or later does not store cardholder data, there is no cardholder data to securely purge as required by PA DSS requirement 2.1. No previous versions of ***Blackbaud NetCommunity*** used encryption; therefore, there is no cryptographic data to securely remove as required by PA DSS requirement 2.7.

When website users enter new credit card information through your website, such as through a donation form, the program automatically sends the data to the ***Blackbaud Payment Service*** for storage and retains the reference number generated by the web service. The user can only access the credit card information entered during the same session on your website.

Your organization can use attributes, notes, and free-text fields to store important information. However, do not use these features to store information such as sensitive authentication data or cardholder data in the program. The abuse or misuse of the program to store this information can leave you vulnerable to an attack by malicious users. If your organization used attributes, notes, or free-text fields to store sensitive authentication data or cardholder data, you must securely delete this data from your database to comply with PCI DSS. For information about how to delete this data, seeSensitive Authentication Data and Cardholder Data Retention on page 2.

Blackbaud NetCommunity does not facilitate the transmission of primary account numbers (PANs) through messaging technology such as email or instant messages. For information about the transmission of cardholder data over open public networks, see Cardholder Data Encryption on page 4.

Merchant Accounts

Blackbaud NetCommunity does not store decrypted login credentials for merchant accounts in the database. The program uses the ***Blackbaud Payment Service*** to store your organization's merchant account information. ***Blackbaud NetCommunity*** can retrieve your merchant account information from the ***Blackbaud Payment Service***.

Website Design

The Frame part and the News Reader part and page element can retrieve information from potentially unverified third-party sources. To comply with PCI DSS, do not use these parts if they reference third-party websites your organization does not trust or cannot verify.

In *Administration*, on the System Options page, you can select the HTML elements to allow in the client-facing HTML editors. To comply with PCI DSS, we recommend you not select **IFRAME** or **SCRIPT** to prevent the use of these tags from within your website.

Integration with The Raiser's Edge

Blackbaud NetCommunity does not send decrypted credit card numbers to ***The Raiser's Edge***. When the program sends transaction information, it includes the reference number generated by the ***Blackbaud Payment Service***. ***The Raiser's Edge*** uses this reference number to identify the credit card number.

To process a donation or membership transaction that includes recurring gift information, you must use ***The Raiser's Edge 7.91*** or later.

Rollback and Uninstall

Before you install any updates, we strongly recommend you back up your database. For information about the update process, see the *Update and New Features Guide*.

If you encounter problems during the installation process, you can cancel the installation before it finishes. After you cancel, the install utility returns your machine to its state before the installation. If you complete the installation process but feel the program may have installed improperly, you can sue the **Add or Remove Programs** utility, available from the Control Panel in *Windows*-based operating systems, to safely uninstall the application.

All installation and update guides are available from the user guides area of our website at https://www.blackbaud.com/training-support/support/howto/raisers-edge#guides.

Services and Protocols

Blackbaud NetCommunity does not require the use of any insecure services or protocols. The services and protocols that ***Blackbaud NetCommunity*** requires are Secure Sockets Layer (SSL) v3 and Hypertext Transfer Protocol Secure (HTTPS). For information about SSL, see Secure Sockets Layer Configuration on page 23.

Secure Sockets Layer Configuration

Secure Sockets Layer (SSL) is a protocol developed by Netscape to transmit private documents via the Internet. SSL uses a public key to encrypt data transferred over a SSL connection. Microsoft *Internet Explorer* and other browsers support SSL. ***Blackbaud NetCommunity*** permits use of the protocol to safely transmit confidential information such as credit card numbers and login information.

To ensure sensitive data is secure over the Internet, you must enable SSL for ***Blackbaud NetCommunity***. To that end, it is important you understand the steps necessary to set up SSL.

Digital Certificates in Internet Information Server

After you acquire a digital certificate, configure it on your NetCommunity web server in *Internet Information Server (IIS)*. To add the new certificate to your web server, follow the directions from Microsoft located at http://support.microsoft.com/kb/228836/. The digital certificate provides the public key that SSL needs to encrypt data. When Blackbaud hosts ***Blackbaud NetCommunity***, the installation engineer assists in the process. For information about how to obtain a digital certificate, see the ***Blackbaud NetCommunity*** System FAQs document provided by Blackbaud Professional Services.

Digital certificates relate to only one root domain name, not an IP address or specific server. For example, you do not need to acquire a certificate for http://www.mydomain.com/netcommunity. Instead, acquire the certificate only for www.mydomain.com. Additionally, when you configure your digital certificate on your default website, do not set the **Require secure channel (SSL)** option in *IIS*. This unnecessarily enables SSL across your entire website.

Configure SSL in Blackbaud NetCommunity

To install ***Blackbaud NetCommunity***, Blackbaud Professional Services follows a series of procedures. If you request that Professional Services enable SSL during your initial implementation, they use these steps. If you do not request Professional Services' assistance, you must complete these on your own.

- After the installation, from *Configuration*, specify whether to require SSL on all pages of your website or only the Administrative site or pages on the Client site that contain sensitive information.
- In *IIS*, the SSLPage.aspx in the NetCommunity virtual directory is modified. This is the only in the instance security settings for the SSL certificate are set to **Require Secure Channel (SSL)**.
- If Blackbaud hosts ***Blackbaud NetCommunity*** for you and your web service is located on your web server in the hosted environment, it must be secure. This requires a separate digital

certificate on that web server for its domain. This is documented in theTechnical Requirements document provided by Blackbaud Professional Services. Additionally, when Blackbaud hosts ***Blackbaud NetCommunity***, Professional Services configures a digital certificate on the NetCommunity web server for your domain.

SSL in Blackbaud NetCommunity

By default, when you enable SSL in ***Blackbaud NetCommunity***, only selected parts are enabled to use SSL. These parts include the User Login, Donation Form, Membership Form, Event Registration Form, Fundraiser, Formatted Text and Images (Secured), and Personal Page Manager. If you set the **RequiresSSL** field to 1 in the **ContentTypes** table in your ***Blackbaud NetCommunity*** database, you can add additional parts as secured.

To secure multiple pages on your website, add an empty Formatted Text and Images (Secured) part to any layout in ***Blackbaud NetCommunity***. This way, any web page that uses the layout is automatically secured.

When a website user is on a page that has a secured part, ***Blackbaud NetCommunity*** dynamically configures each image URL, URLs defined in parts, and document file URLs to "https". When a user navigates to any one page that contains an SSL part, the small lock appears on the browser. ***Blackbaud NetCommunity*** maintains this secured environment to the next page the user navigates to. It does not matter whether it has an SSL-enabled part. Any data transmitted from these secured pages is encrypted.

Configure SSL Settings in the Windows Registry

Warning: If you modify the registry file incorrectly, serious problems may occur. Before you edit the registry, we strongly recommend you create a backup so you can restore the file if necessary. For information about how to back up and restore the registry file, see http://support.microsoft.com/kb/322756.

To ensure the safe transfer of sensitive credit card data from ***Blackbaud NetCommunity***, you must configure your SSL settings to enforce strong encryption. To prevent the weak encryption of credit card information, edit these SCHANNEL keys in your *Windows* registry panel:

[HKEY_LOCAL_ MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56] “Enabled”=dword:00000000

[HKEY_LOCAL_ MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 40\128] “Enabled”=dword:00000000

[HKEY_LOCAL_ MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56\128] “Enabled”=dword:00000000

[HKEY_LOCAL_ MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\MD5]

“Enabled”=dword:00000000

For more information about how to adjust the Schannel.dll file to restrict cryptography and protocols, see http://support.microsoft.com/kb/245030.

Additional SSL Information

To avoid mixing secure domains with non-secure content, you must modify ***Blackbaud NetCommunity*** background URLs on Menu parts or in your custom CSS to "https://" (instead of "http://"). In addition, we recommend you modify any javascript URLs used in Formatted Text and Images parts to "https://".

In these situations, you can set URLs used to relative URLs. For example, for background images in your styles view.image?Id= 478 in the URL can be used in a style, such as background-image:url (view.image?Id= 478);. In this example, the URL references an image in *Images*. This is resolved to the correct domain during rendering, regardless of security.

We recommend that you sparingly use fixed URLs in styles and javascript because SSL retrieves the images every time it loads a fixed page. It does not matter whether the page is secure.

If you do not enable SSL on the ***Blackbaud NetCommunity*** Administrative site, but you do enable the client site web pages, mixed mode messages and SSL redirect messages may appear when you switch between administration pages and your website pages.

If you plan to host objects such as streaming media files or iframes that reference files hosted elsewhere, we recommend you consider the issue of combining secure and non-secure content. A non-secure page in an iframe on the same page as a secured ***Blackbaud NetCommunity*** web page is considered mixed content. In each instance, during the design of your site, we recommend you located mixed areas of content together on the same NetCommunity web server or secured by its own digital certificate.