PayPoint Gateway Overview
NC Office of the State Controller
Revised February 1, 2015

What is the PayPoint Gateway?
PayPoint is a web capture gateway solution available from First Data Government Solutions (FDGS) through SunTrust Merchant Services (STMS). The service is an optional gateway service that may be subscribed to under OSC's master contract with STMS.

What are the two primary payment processes offered by PayPoint?
PayPoint's consumer interface feature offers an agency the ability to accept online payments from citizens (consumers) and process them through one of two options. The option utilized depends upon who will authenticate the attempted payment, the agency or PayPoint. Under each option, the citizen accesses the agency's website first.

- Authentication performed by agency – Agency authenticates an attempted payment to an internal database of open transactions, and if there is a match, the citizen is then redirected to PayPoint allowing him/her to select the payment method to complete the transaction.
- Authentication performed by PayPoint – From the agency's website, the citizen is initially redirected to a PayPoint hosted website, where the authentication process is performed against a database maintained at PayPoint, and if there is a match, the citizen can select the payment method to complete the transaction.

How is PayPoint made aware of the open transaction(s) for which a payment may be initiated? This will depend upon who performs the authentication function, the agency or PayPoint.

- Authentication performed by agency – The Advanced Query String process (real-time secure Web HTTP) is utilized. Upon a successful match on the agency's website, the agency passes the open transaction data to PayPoint, where the transaction can then be completed by the citizen selecting his/her payment option. PayPoint does not maintain a database of open transactions, as it only displays and acts upon the single query string message submitted by the agency.
- Authentication performed by PayPoint – The Data File Upload process (a batch file upload) is utilized. The agency submits to PayPoint a file containing all open transactions though a secure FTP batch file upload process. The agency must keep the open transactions file updated in order for PayPoint to be able to authenticate attempted payments. PayPoint retains each open transaction in the database flagged as open until the transaction is either paid, or later deleted by the agency. Additionally, at any time through the Admin feature, the agency can manually update the open transactions file in the database maintained at PayPoint (add or delete an open transaction). (The batch file upload made through the Consumer Interface module is not to be confused with the API-Batch File process associated with the API module referenced in PayPoint's manuals.)

How is the agency made aware of successful payments initiated through PayPoint?
There are three possible ways of receiving the payment results, depending upon which interface option is utilized for submitting open transaction data to PayPoint (Refer to page 10 for further discussion.):

- Posting File - Agency downloads a posting file, normally the next business day, either manually or via an automated process. (Applies to both methods of submitting open transaction data to PayPoint.)
- Detail Payment Transaction Report – Agency runs and retrieves transaction reports through the Admin screen. (Applies to both methods of submitting open transaction data to PayPoint.)
- Query String Return Call – For each query string (Query Call) submitted to PayPoint, PayPoint communicates back to the agency's return URL (Return Call), upon either the success or failure of the attempted payment. This Return Call is real-time and allows the agency to update its database of open transactions as payments are made at PayPoint. (Applies only to the Advanced Query String method of submitting open transaction data to PayPoint.)

Comparison of the two methods of transmitting open transaction data to PayPoint
Consultation with OSC and/or First Data and consideration of the agency's needs are required in order to select the appropriate method. The two methods are: 1) Advanced Query String (Secure Web HTTP); and 2) Data File Upload. Below is a comparison of the two methods associated with the Consumer Interface feature.

Comparison of Two Transmission Methods w/ Consumer Interface Feature					
Method	Real Time	Authenti-cation	Agency's Role	Pros	Cons
Advanced Query String **(Secure WEB HTTP)**	Yes	On Agency's website	Maintains agency website for authentication of A/R (invoice ID and amount) before being forwarded to PayPoint for selection of payment method Invoice data is transferred to PayPoint to be displayed to payer only when payer's online-entered data is authenticated by agency, thereby allowing payer to select payment method Agency receives response real-time from PayPoint when payment is authorized/rejected	Database of open transactions does not have to be maintained and be kept updated on PayPoint's servers Receipt of payment notification from PayPoint is real-time via returned query string	Agency has to develop web form to capture transaction on agency's website Agency has to develop program to authenticate against agency-maintained database, and if a match, submit query string to PayPoint Agency has to program to receive Return Call results
Data File Upload **(Batch Data File)**	No	On PayPoint website	Create open A/R transaction file and upload to PayPoint, keeping database maintained at PayPoint updated Upload can be via FTP to First Data's secure FTP server or through PayPoint's Admin screen Agency's website has a link to PayPoint, where payer enters all payment data, resulting in PayPoint performing authentication based on open transactions database, and offering payment method to payer Files must be created in a format specific to the agency. Data encryption software must be used such as WinZip or others that are SSL 128 bit compatible.	No programming needed for agency authentication Receipt of payment notification can be real time, but only if an optional "Post Authorization plug-in" module is obtained (customization required)	Database at PayPoint must be maintained and kept updated Requires Secure FTP upload, generally daily Receipt of payment notification from PayPoint not real-time, only when retrieval of posting file is downloaded, or transaction data viewed via Admin site

What features are available via the two PayPoint Consumer Interface Option?

Advanced Query String			
Standard Features			**PayPoint Fee**
	Payment Gateway	Application hosted by First Data	$.08 / Trans
	Consumer Interface	Payments entered on PayPoint via Web	$.02 / Trans
	Database	On agency's website	N/A
	Authentication	On agency's website	N/A
	Portal Builder	Used by agency to design site	Included
	Admin Site	Used by agency to perform variety of functions	Included
	Virtual Terminal	Agency can key transactions via Admin screen	Included
	Posting File	Downloadable (completed transactions)	Included
		Total Basic Fees Per Transaction	**$.10**
	For transactions entered via PayPoint's Admin site (Virtual Terminal), the $.10 per transaction fee does not apply.		
Optional Features			
	Summary Presentment	Not normally applicable under Query String	N/A
	Enrollment	Not normally applicable under Query String	N/A

Data File Upload			
Standard Features			**PayPoint Fee**
	Payment Gateway	Application hosted by First Data	$.08 / Trans
	Consumer Interface	Payments entered on PayPoint via Web	$.02 / Trans
	Database	On PayPoint's website	Included
	Authentication	On PayPoint's website	$.05
	Portal Builder	Used by agency to design site	Included
	Admin Site	Used by agency to perform variety of functions	Included
	Virtual Terminal	Agency can key transactions via Admin site	Included
	Posting File	Downloadable (completed transactions)	Included
		Total Basic Fees Per Transaction	**$.15**
	For transactions entered via PayPoint's Admin site (Virtual Terminal), the $.10 per transaction fee does not apply.		
Optional Features	Features below **not** used with Query String		
	Summary Presentment	Users can be displayed both unpaid and paid invoices. (With Registration/Enrollment feature only.)	$.10 / trans
	Registration/Enrollment	Users can be enrolled on PayPoint, allowing users' self-service to update user's profile, payment method(s), ability to view history of prior transactions, and to initiate reoccurring payments (if offered)	$.02 per enrollment
	Reoccurring	User can be setup to schedule payments to be auto-made against card or bank account on file	With enrollment only

What are the major benefits of PayPoint?
- PayPoint has a consumer interface, which has a web capture feature as part of the solution.
- Multiple Payment Options – PayPoint allows the site visitor to select one of two payment options – credit/debit card or ACH bank draft (E-Check)

When is PayPoint suitable for an agency?
- Agency desires to accept payments online, but does not have the internal resources and/or expertise to develop a comprehensive in-house web capture application
- Agency desires to utilize a third-party gateway service provider to minimize (but not completely avoid) applicability of the PCI Data Security Standard requirements, primarily by avoiding the agency ever having to store cardholder data in the agency's database
- Agency desires to offer both the ACH bank draft payment option (E-Check), in addition to the card option; or to just offer one of the options
- Agency has outstanding invoices (accounts receivable transactions) associated with payers, which are conducive to being authenticated online-real time, either on the agency's website or on PayPoint's website, before being accepted and transacted via PayPoint

Is PayPoint the gateway of choice for an agency needing gateway services?
OSC's policy states, "Agencies requiring a gateway service in order to participate in the MSA(s) may select a secure gateway service of its choosing, provided it acquires approval from OSC and adheres to all applicable procurement requirements."

PayPoint is just one of several third-party gateways that an agency may elect to utilize. Some third-party gateways specialize in certain types of transactions that are more suitable for the agency. For example, some specialize in tuition payments and some in online reservations. The agency must also consider which gateway is compatible with its accounting system (e.g., PeopleSoft or Banner for the universities and Datatel for the community colleges). While there are two gateway capture solutions available through OSC's master contract with STMS (PayPoint and First Data Global Gateway), an agency is not required to utilize either, just as it is not required to obtain POS terminals from STMS. Utilization of PayPoint does not require the agency having to issue an RFP.

When is the PayPoint gateway service more appropriate to use than the Global Gateway?
PayPoint is a recommended solution for an agency that needs a "consumer interface" feature. The First Data Global Gateway solution (formerly called YourPay) offered by STMS does not have a web consumer interface feature. PayPoint is more suitable for agencies that have accounts receivable transactions that have been invoiced to a payer and can be authenticated online before being paid (either by the agency or by PayPoint). PayPoint is also suitable when the agency desires to offer bank draft (E-check) as a payment option, in addition to the credit card option; or to only offer the E-check option (suitable for large payment transactions).

Does PayPoint accommodate card-present transactions and MOTO?
Yes, in addition to accommodating web-initiated payments by the consumer, PayPoint can also function as a "virtual terminal" solution, with the agency initiating the payments through the agency's Admin PC screen. This could be for walk-ins (card-present) or for mail orders / telephone orders (MOTO). The normal capture method would be for the agency personnel to key the cardholder data or check data (for bank drafts) on the Admin PC screen while connected to the PayPoint website in a secure session. PayPoint provides for a customer receipt to be printed, which can be provided to the payer (in person, or emailed). Card capture via a magnetic stripe reader connected to the agency's PC is an alternative to the agency personnel keying the card data onto the PC screen. For transactions entered through the Admin screen, the $.10 per transaction Consumer Interface fee does not apply.

Using a gateway as a virtual terminal does have certain PCI Data Security compliance implications, as cardholder data is being "processed" at the agency's location, via a device connected to the Internet. The degree of implications depends partially upon rather the PC is segmented from other agency servers or not. Agencies utilizing PayPoint as a virtual terminal must have the associated external IP addresses enrolled in

Coalfire so that the external facing (public) IP addresses can undergo quarterly vulnerability scanning.

Are there other ways of utilizing PayPoint involving an API solution?
While PayPoint does offer an API (Application Programming Interface) solution, which does not utilize the Consumer Interface feature, it is not the recommended utilization of PayPoint for agencies, as it requires more agency website maintenance and greater PCI Data Security compliance implications

What type of technical knowledge must an agency have?
IT expertise that is needed by an agency will depend largely upon the type of interfacing of transaction data between the agency's transaction database and the PayPoint application. Minimal technical knowledge is needed in developing the web portal on the PayPoint server through the consumer payment module. However, IT staff will be involved in the setup of the upload process of open transactions to PayPoint [i.e., either: 1) Advanced Query String involving Web HTTP; or 2) Data upload/download files]. Knowledge of FTP file upload/download (ASCII), and advanced query strings are helpful when determining which methods of interfacing data (to and from PayPoint) are to be utilized. There are several methods of uploading and downloading of data to/from PayPoint available. The handling of data received from PayPoint (posting file or detail transaction report) can either be interfaced or manually posted. A review of PayPoint's Integration Guides will give an agency an idea of the type of technical expertise needed.

How is the consumer payments website designed?
Using the Consumer Payments design toolkit (portal builder), for each payment application, the agency logs-on to PayPoint through the Admin screen and creates its own webpage. The toolkit allows for the agency to use its own agency logo, pick a theme, fonts, colors, headers, footers, and establish rules for the particular payment. The site can be disabled as needed, such as to perform maintenance.

How does PayPoint handle the agency's logo?
The PayPoint application links to the agency's logo (gif or jpg) maintained on a secure server maintained by either: 1) the State agency, or 2) First Data. If the URL link, which is provided during the setup, is not to a secure server (https), the consumers will get a security warning message when initiating payments. Therefore, unless the agency has a secure server to house the logo, the agency must provide the GIF or JPG logo to First Data for hosting.

Are there any start-up fees for the agency?
As of February 1, 2015 when the terms of our new contract with STMS went into effect, there are no implementation fees.

Are there any on-going transaction fees?
STMS Amendment Number 2 contains the fee schedule. Transaction fees will vary based upon which of the two transaction interface options are utilized, and which additional features are utilized. The two basic per transaction fees that apply are: 1) Gateway transaction fee - $.08; and 2) Consumer Interface surcharge fee - $.02. The $.02 surcharge does not apply for transactions entered via the agency's Admin screen. If the Data File Upload interface feature is used, which requires authentication on PayPoint's website (instead of on the agency's website), an additional $.05 authentication/challenge fee would apply.

What additional "other" on-going transaction fees could apply?
A "Summary Presentment Surcharge" fee of $.10 per transaction would apply if the agency wishes for payers to be displayed billing data (both paid and unpaid invoices) associated with the payer's ID. An "Enrollment" fee of $.02 per registration/enrollment would apply if the agency wishes for the payers to be able to pre-enroll and maintain their own online profile (see below). The PayPoint fees would be in addition to any fees associated with processing card transactions through STMS, which involve interchange and assessment fees charged by the card brands.

Are fees for PayPoint services separate from fees for processing card transactions?
Yes. Services for fees associated with PayPoint will be invoiced by First Data Government Solutions, while services for processing card transactions will be invoiced by SunTrust Merchant Services (STMS).

Is there a payer Registration / Enrollment feature?
PayPoint offers the ability for payers to register in PayPoint, establishing an online payer profile. This feature is available at either the agency or application level. There are both advantages and disadvantages to offering this option. Advantages include: 1) Payer has the ability to view history of previous transactions; 2) to store the card number or bank account number it desires to be used when making payments; 3) to enroll in re-occurring payments; and 4) to receive email confirmations when payments are made. Disadvantages include: 1) UserID and password maintenance must be considered; 2) risk associated with expired cards or changed bank accounts must be considered; 3) payer may confuse PayPoint profile with their profile maintained on the agency's records; 4) payer must logon to PayPoint whenever making a payment, even if already authenticated at the agency's website; and 5) the feature cannot be used in conjunction with the query string method.

This feature may be appropriate if re-occurring payments are due from a payer (i.e., payment schedule is established), and then only if the Data File Upload method is used. If the registration/enrollment feature is chosen, a separate application is required, separate from the application for payers not being pre-enrolled.

Are there any Interactive Voice Response (IVR) fees?
PayPoint accommodates IVR, but there is no perceived demand for this service. Initially, PayPoint will be used primarily for "card-not-present" transactions, and ACH bank drafts (E-Checks) initiated through the Web, as well as via MOTO (mail order telephone order). If you choose to use IVR, the fee is $.08/minute.

How are bank drafts (E-Checks) processed through PayPoint?
While card transactions are routed through STMS for collection and settlement, bank draft transactions (also referred to as E-Checks) are routed through TeleCheck, a business unit of First Data. TeleCheck functions as the ACH originating bank, with ACH debits being submitted against the payer's bank account, and the proceeds being credited to the agency's designated bank account. The agency's designated bank account normally is the same ZBA account the agency has with the State Treasurer for the settlement of its credit card transactions (at Wells Fargo for agencies).

Are there any fees associated with originating ACH bank drafts?
No, there are not any ACH related fees beyond the basic PayPoint per transaction fees. Should the payer select the bank draft option to initiate a payment (referred to as an "E-Check"), the agency avoids the interchange fees associated with processing merchant cards.

Can an agency elect to only offer the E-Check payment option for a particular application?
Yes, this may be appropriate when the average transaction amount for a particular application (or set of payers) is normally very large, and the agency does not want to incur the interchange fee associated with a card transaction. (Interchange fees are based on a percentage of the amount of a card transaction.)

When an open invoice transaction is displayed to a payer, can the payer change the amount field?
Any of the fields presented to a payer on the "Make Payment Screen" can be coded to be either editable or non-editable. Making the amount field editable would allow a partial payment (not generally recommended).

When are funds credited to the agency's bank account maintained with the State Treasurer?
In the case of both card transactions and bank drafts (E-checks), funds are credited to the agency's dedicated bank account at Wells Fargo, one banking day after the transaction date. Exception is in case Amex or Discover are accepted, which has an additional one-day delay. Although the E-Check transactions will be credited to the agency's bank account separate from the card transactions, the net total of both set of transactions will be swept to the State Treasurer's account as one amount, thereby requiring the agency to certify on CMCS the single amount transferred (representing all transaction activity combined).

What tools are used to perform the funds reconciliation function?
The agency will utilize several online reporting tools to perform the reconciliation function. In the case of entities depositing funds with the State Treasurer, the dedicated sub-ZBA bank account assigned by the State Treasurer (with associated CIT account number) will be utilized to account for all funds received (as

well as debits for returns and chargebacks) for the various transactions.

Funds will be received from: 1) from STMS credit card and debit card transactions; and 2) from TeleCheck for ACH (E-Check) transactions. A daily settlement will be received from each of these two sources on a daily basis, and credited to the agency's designated ZBA bank account established with the State Treasurer. Online tools to be utilized to view what is expected are ClientLine (for cards) and PayPoint reports (for cards and E-Checks). E-Check transactions cannot be viewed on ClientLine. The online tool to be utilized to view the funds actually received and credited to the bank account for all transactions is Wells Fargo CEO.

On a daily basis, the agency's dedicated ZBA account at Wells Fargo will have the following transactions, for each application: 1) daily total of Visa/MasterCard transactions; 2) daily total of E-Check transactions; 3) individual card chargebacks; 4) individual bank draft returns. The net total of each day's transactions (one amount) is swept from the agency's dedicated bank account to the State Treasurer's bank account, which is the amount the agency is to certify via OSC's Cash Management System (CMCS), using the agency's CIT number assigned by the State Treasurer. The agency is normally assigned one dedicated bank account by the State Treasurer for all applications, and has access to the bank account via the online Wells Fargo CEO portal. The agency has access to view the CIT account transaction activity via the State Treasurer's Core Banking System.

What are the tiered pricing fees contained in Amendment No. 2?
The basic PayPoint gateway transaction fee starts at $.20, which applies if the monthly transaction volume, for all agencies combined, is 50,000 transactions or less. The fee schedule allows for a tiered reduction should the monthly total transaction volume, for all agencies combined, exceed 50,000 transactions. OSC will notify the participating agencies should a new threshold be reached.

Does PayPoint accommodate a convenience fee being levied against a payer?
Yes. There are two options available: 1) Fee may be levied by the agency and collected by the agency; or 2) Fee may be levied by First Data Government Solutions (FDGS) and retained by FDGS. There are implications for levying a convenience fee, depending upon which card brands are accepted. For example Visa only allows a flat fee per transaction. The levying of convenience fees must be approved by OSMB and ITS pursuant to G.S. 66-58.12, even if the fee is retained by FDGS.

Does PayPoint accommodate Address Verification and/or Security Code Verifications?
Yes, AVS and CVV2 are accommodated. However, using AVS and CVV2 increases the rejection rate of valid card number and expiration date being submitted online. Should the agency authenticate each payer (e.g., through a pre-assigned invoice number or vendor ID), these features could be waived, as the risk of a stolen card number being submitted is minimal. If the agency does not authenticate the payer, the CVV2 code verification feature should be used. There is an additional $.02 per transaction fee levied by STMS if AVS or CVV2 is utilized. Additionally, MasterCard levies a fee of $.0075 per transaction if AVS is utilized, while Discover levies a $.50 per transaction fee if AVS (for both street address and zip code) is not utilized. The feature is selected when the Boarding Form is completed. Refer to OSC's document, "Fraud Detection Services" for more information.

What types of payments can be made through PayPoint?
Two types of merchant cards are typically accepted: 1) credit cards; and 2) signature debit cards (with Visa/MC logo). In addition, ACH bank drafts (referred to as E-Checks) can be accepted.

What are and can PIN-less debit cards be accepted?
A PIN debit card is issued by a bank and generally requires authorization by the entering of a 4-digit PIN. The transaction results in the payment being deducted directly from the consumer's bank account. PIN debit cards bearing the mark of NYCE, STAR, and PULSE (and may or may not bear a Visa or MC logo) are eligible for a government to be accepted without having to acquire the 4-digit PIN, but a special enrollment is necessary through STMS. When taken in this manner, the card is referred to as a "PIN-less debit card" (not the same as a signature debit card). Selecting this feature is not typical for online payments. The feature can be added to PayPoint during the initial setup (which can delay the implementation), or it can be added at a later date.

What card brands can be accepted?
All card brands can be accepted through PayPoint. Visa and MasterCard are eligible to be accepted as part of the contract with STMS. In order for American Express or Discover to be accepted, the agency must enroll in the services offered under master contracts that OSC has with those card brands. It should be noted that settlement of funds for American Express is two days instead of one day. The settlement of funds for ACH bank drafts (E-checks) is one day.

How is the authentication of payments performed?
All payments should be authenticated as being one that is an open transaction in the agency's accounts receivable database before the payer is allowed to initiate the payment. The authentication can be performed: 1) on the agency's website if the Advanced Query String interface option is utilized; or 2) on PayPoint's website if the Data File Upload interface option is utilized. PayPoint refers to the authentication process as "challenge data." If the authentication (challenge) is performed at the PayPoint website, the agency must have previously uploaded the open transactions to PayPoint. In order to authenticate a payment, the payer should be prompted to enter at least two elements associated with an open transaction, such as invoice number (or license number) and amount of the obligation. These elements are established when the payment

- application is setup. The payer will normally be aware of the two challenge elements as a result of an invoice having previously been submitted to the payer. If the payer does not enter the appropriate challenge data, the open transaction cannot be retrieved and displayed, and the payment cannot be
- initiated, with an error message being displayed back to the person. Whatever challenge data is selected, the data will be displayed on PayPoint for the payer to view before making the payment.

     Some agencies may have a website that already authenticates users accessing its website for purposes other than making payments. Some may even utilize NCID. Such agency-maintained website authentication process can be used in conjunction with allowing the payer to select an open payment invoice.

Can free-form payments be made – where there is no outstanding A/R transaction?
An agency may establish a separate application where free-form payments can be submitted. In such case, the application must be set up using the Registration/Enrollment feature. Once an enrolled user logs on to PayPoint using their email address and assigned password, he/she can then further be authenticated by being presented a challenge data element (e.g., Tax ID or license number). Associated with this challenge element can be any type of payment, such as an amount field (blank or set amount) (editable or non-editable), and a field for payment description (set or editable). The challenge data is submitted to PayPoint via the Data File Upload method. The query string method is not associated with this type of arrangement.

Why is authentication necessary?
Allowing a web user to initiate a payment using PayPoint without being authenticated in some way is not permitted, as an un-authenticated web user could initiate fraudulent card payments or bank draft payments against an account not belonging to them. A common scheme is for individuals to use unsuspecting websites to test the validity of stolen credit card numbers.

What are the two Data File Upload methods available to send a file to PayPoint?
"Manage Uploads" option under "Data Management" through the Admin Screen – User can browse its own file directories to locate a file, and then upload it to PayPoint. Recommended for smaller files under 100 MB. Secure FTP site at First Data – Recommended for larger files. Requires file to be encrypted. Transmission can be manual or automated.

What are the stages of a payment being made online by a payer?
There are five stages of a transaction, with each stage having a unique screen:
- Challenge Screen – Payment data entered (On agency's website instead of PayPoint if Query String option is utilized)
- Bill Review Screen – If challenge data matches, the invoice to be paid is displayed
- Make Payment Screen – The payer selects the method of payment. Any additional info the agency wishes to capture, can also be required to be entered by the payer.
- Payment Review Screen – Displays payment data entered, and allows payer to go back to the Make

Payment screen to make any corrections
- Payment Complete Screen – Once the payment has been processed, the Payment Complete screen displays the transaction results and will display a confirmation number, if successful. If a transaction is not successful, this screen will display payment rejection reasons. Upon exiting the Payment Complete screen, the payer is redirected back to the agency's website.

For each of the above screens on PayPoint, the agency designs the screen, by placing text instructions in both the header and the footer. There is also a "Page Footer" which shows at the bottom of all pages (not to be confused with the "screen footer," which can be different for each screen. Contained in the Page Footer can be links to the agency's website containing info such as, "Contact Us" and "Privacy Statement."

Is the payer provided a confirmation of the payment?
Yes, upon successfully initiating a payment online, the payer will be provided a confirmation screen, which can be printed. Additionally, for payments entered by the agency through the Admin screen, the agency's administrator can generate a confirmation which can be emailed or mailed to the payer. Should the Registration/Enrollment feature be utilized, the payer will receive a confirmation via email.

Can an email confirmation be sent to the payer for an online payment?
The payer is provided a confirmation screen which he/she can print. In addition, an email confirmation can automatically be sent at the time the payment is made, but only if the "registration/enrollment" feature is utilized.

What type of information is passed from PayPoint to the agency upon completion of a payment?
For applications using the Data File Upload method, there are two ways of receiving "payment results:" 1) Posting file; and 2) Transaction reports. For applications using the Query String method, a Query String Return Call is received by the agency, in addition to the two methods above. The agency can use either or a combination of these methods to update its accounts receivable database. Note that funds are not actually received until one banking day after the payment is initiated (the same day the posting file is received).

For both interfacing options (Query String or Data File Upload), information pertaining to "payment results" is available to the agency via a "posting file," generally the next business day. The posting file can be: 1) downloaded manually via the agency's Admin screen; or 2) downloaded from First Data's secure FTP site (manually or scheduled). The posting file is available in various formats if downloaded from the PayPoint Admin site. If downloaded from First Data's FTP site, the file is an ASCII text file (encrypted). Information on the posting file has data that can be used to update the agency's A/R database. See page 150 of the PayPoint Merchant Integration Guide (Version 2.5.0) for specifications on the "posting file." In addition, the agency can create customized reports (e.g., Detail Transaction Report) using the Search/Report feature and export the file in various formats (including Excel).

If the "Advanced Query String" interface option is utilized, an electronic response (Return Call) can be sent to the agency real time upon the completion of a payment transaction. If the "Data File Upload" interface option is utilized to submit open transactions to PayPoint, real-time updating of the payment results is not the norm, as updating is performed by downloading a posting file on a scheduled basis, or by retrieving detail transaction reports.

However, a customized solution is available if real time updating of payment results is required in conjunction with the Data File Upload option of submitting open transactions to PayPoint. This "Post Authorization plug-in" feature incurs additional customization costs. Consultation with First Data would be needed if this option were to be pursued.

What is the Reference field?
The reference field is a 254 character field associated with a payment transaction that can contain information about a payment beyond the standard information fields associated with a transaction. The reference field can contain multiple elements of information to identify the transaction. For example, it can

contain invoice number, license number, or other fields that the payer has been prompted to enter on a capture screen. The reference field is contained on the posting file downloadable from PayPoint or from First Data's secure FTP site, which the agency can use to map to its database.

How are payments that are in the A/R database cleared if a payer pays the agency directly by check instead of via PayPoint?
If the Data File Upload option is being utilized (where PayPoint performs the authentication function), the agency would update the records within PayPoint by sending updated files to PayPoint on a daily basis with current status information. The new file could either delete the previously submitted file, or mark the item with a new status of paid.

What are the three hierarchy levels associated with a payment?
A payment is processed/stored/searched under the following hierarchy: 1) Site; 2) Agency; 3) Application. The "site" will always be ""NCOSC – NC Office of State Controller." The "agency" will always be (your agency). There can be multiple "applications" under (your agency), with each application being assigned a three digit number. You will only have access at the Agency level, and can assign specific access to individual applications under the Agency, based on the roles and access levels needed by your staff.

How are transactions identified in PayPoint?
Within each payment application, a newly created transaction (primary payment) is initially assigned a "transaction ID." Each primary payment transaction may have several subsequent actions associated with that transaction, such as, cancellation, or chargeback. Each action (payment type) associated with the transaction ID has its own unique "confirmation number." Upon viewing a transaction ID, you can drill down to view each "action" associated with the payment by using the confirmation number.

Do transaction records have different status codes?
Yes, a transaction could be "successful - payment pending," or "settlement complete." Once a payer initiates a payment, PayPoint accumulates all payments and submits them for payment (either to STMS for cards or to TeleCheck for E-Checks) at an established nightly cut-off time. Up to the point the transaction is settled, the transaction can be canceled. The recommended cut-off time is 5:00 p.m. Eastern Time, in order to coincide with TeleCheck' s daily cut-off time for next-day funding. The cut-off time is established when the application is set up.

Can transactions be refunded?
To initiate a refund, there must be a previously entered transaction, either a card transaction or an E-Check transaction. A refund entered against a previous card transaction (which may be for the full amount or a partial amount) initiates a credit back to the card, and results in funds being transferred from the agency's bank account to the cardholder's card account. A refund entered against a previous E-Check transaction (which normally is for the full amount) does not result in the movement of funds, as it only results in the change of the transaction's status. If the agency learns of an E-Check return from the bank, the agency can log on to the Admin site and record the transaction as a return. E-Check returns will are associated with bank drafts returned due to either the bank account that was provided is invalid, or the payer's bank account had insufficient funds.

What is a chargeback?
Chargebacks only apply to card transactions. Chargebacks entered by the agency only results in the change of the transaction status, not the movement of funds. A chargeback entry is used when the agency learns that STMS has debited the agency's bank account, for a previously settled card transaction.

Can duplicate payments be prevented?
During an application's setup, the system can be coded to not allow duplicate payments within a certain time frame. The time frame chosen can be within minutes or within days.

Can a web payer's IP address be viewed?
Yes, each transaction has a "source ID." In the case of a web payment, this would be the payer's IP

address, which could be useful in detecting fraud transactions.

Are multiple languages supported?
Currently, both English and Spanish are supported.

How does the PCI Data Security Standard apply to PayPoint?
STMS Amendment Number 2 has a stipulation that requires First Data to acknowledge that as a service provider, it is responsible for the security of cardholder data it possesses, as required by Requirement 12.8 of the PCI Data Security Standard (PCI DSS). How the agency uses PayPoint will determine which Self Assessment Questionnaire (SAQ) the agency must complete. If the Admin screen will never be used by the agency to initiate card payments on behalf of a payer (functioning as a virtual terminal) vulnerability scanning of the agency's external facing IP addresses is not required, and SAQ-A applies.

Agencies utilizing PayPoint as a virtual terminal (entering card transactions via the Admin screen) must have the associated external facing (public) IP addresses enrolled in Coalfire so that the IP addresses can undergo quarterly vulnerability scanning. The completion of SAQ C is required if: 1) data is not stored in electronic format; and 2) the PC is a stand-alone-terminal not connected to any other system. Otherwise, the completion of SAQ-D is required.

Does the International ACH Transaction (IAT) Rule apply to the E-Check transactions?
Yes. Since the agency will be accepting E-Check transactions, which is an Automated Clearing House (ACH) debit online, the agency must perform its due diligence efforts to prevent the website from being used as a means to originate ACH transactions against a bank account funded with moneys from a foreign bank. The agency must include language in its website's Privacy Policy to address the IAT rules. See the Sample IAT Privacy Statement.

In the State's setup structure, who functions as the Corporate Site?
The Office of the State Controller (NCOSC) functions as the corporate site, and each agency functions as a participant under the site. Each agency can then have multiple payment applications (or multiple divisions).

How does the administrator function work?
The OSC has an administrator with the ability to setup an administrator at each agency, providing him/her certain administrator rights. Each agency's administrator then has the ability to: 1) set up applications; and 2) set up users within the agency. The agency administrator also assigns roles to users.

What types of reports are available?
There are nine standard reports available. In addition, an agency can create customized reports using templates. The reports are available in various formats, including cvc and XML. The reports can be exported to Excel if desired.

Who is responsible for the help desk function?
FDGS provides help desk services to an <u>agency</u> regarding the operation of PayPoint, and can be reached at 877-869-0860, or by emailing paysupport@firstdata.com. However, each agency is responsible for maintaining its own help desk to deal with problems encountered by payers.

Does an agency have to execute an agreement in order to subscribe to PayPoint?
The agency must be a participant under the OSC's master contract with STMS for merchant card processing services, which requires the agency to have previously executed a "Schedule E – Agency Participation Agreement." The revised Schedule E has a separate section at the end which the agency would have to complete in order to subscribe to the PayPoint optional service. An agency must re-execute Schedule E if it is an existing participant, and now desires to subscribe to the PayPoint service.

Does the agency have to establish a separate merchant number for card transactions?
Yes, a <u>separate</u> merchant number is needed for <u>each application</u> that will accept cards, as merchant numbers are normally associated with a particular capture method and are needed to identify the

Visa/Master card daily settlements for a particular application. Merchant numbers do not apply to E-Check transactions, but a TeleCheck number is assigned to each application, similar to a merchant number.

What is the implementation process?
The implementation phases include: 1) Analysis of features/interfaces to be utilized; 2) registration and setup; 3) complete PayPoint Boarding form 4) interface development; 5) testing; 6) certification; and 7) production. Once the interface option is chosen (Query String or Data File Upload), there is a boarding form that an agency must complete upon enrolling. A separate boarding form is to be completed for each "payment application" the agency will be accepting online. An agency will typically have multiple payment applications (e.g., license renewal, permit fees, fines, etc.).

What is the UAT Region?
After selecting the upload interface for an application, and completing the Boarding Form, the PayPoint project manager will setup the application in PayPoint's "User Acceptance Test" (UAT) region. The application will be similar to what will eventually be in the Production Region, but not necessarily the same. The UAT region will allow the agency to perform three modes: 1) Testing; 2) Certification; and 3) Production. The "production mode" is not really true production, as it is within the UAT Region.

What is the Production Region?
After performing all three modes within the UAT Region, the agency will be setup in the Production Region, based on the Boarding Form completed by the agency, but modified according to any necessary changes identified necessary while testing in the UAT Region. The same three modes (testing, certification, and production) will be performed in the Production Region. However, during the certification mode, live $1.00 transactions will be initiated against real card and bank accounts.

Are there any PayPoint Integration / User Manuals?
Yes. Be sure to refer to the most current version. The most current versions of the manuals are available through First Data's online E-Room / Product Room / Documents. (UserID and password are available from OSC.). Below are some common topics:

Topic	PayPoint Merchant Integration Guide V.2.5.0	Consumer Payments Integration Guide V. 2.5	PayPoint User's Guide Version 2.5.2
Interfacing Options		Pages 81-84	
Query String Option		Page 82 +, 106 +, 116-119	
Data File Upload Option		Page 81 +	
Posting Files	Page 150 +		Page 165
Registration/Enrollment		Page 7 +, 58, 70 +	Page 138 +
Convenience Fees		Page 66	Page 85 +
Reports			Page 110 +

Note that the "PayPoint Merchant Integration Guide" contains info regarding a client that would be using PayPoint with an "API solution," which does not involve the Consumer Interface feature. Much of this info does not apply to NC agencies. (The batch file upload made through the Consumer Interface module is not to be confused with the API-Batch File process associated with the API module referenced in PayPoint's manuals.)