State of Wisconsin
Enterprise Banking Services Contract
Appendix 2 – Electronic Payment Gateway Service

Table of Contents

1.0 GENERAL OVERVIEW OF SERVICES

The Contractor shall provide services related to the processing of incoming electronic payments (hereafter referred to as "Electronic Payment Gateway Services"). The services to be provided are described in this contract appendix. The Contractor shall provide a gateway system that accepts credit card, debit card, pin-less debit card and Automated Clearing House (ACH) Electronic Payment Gateway Services for payments made through the Internet and through Interactive Voice Response (IVR).

2.0 TECHNICAL MODEL FOR INTERNET PAYMENTS

Definitions

Authentication - the process by which a web user submits identifying data (e.g. userID and password) and by which that data is corroborated against pre-existing, verified data.

Authorization

- For ACH payments: the process by which the Payer agrees to the Biller's terms and conditions to allow payments to be withdrawn from a Payer's account.

- For credit/debit card payments: the process by which the available card balance is compared to the payment amount. If the card balance is sufficient, a "hold" is placed upon the Payer's card balance for the amount of the payment.

Biller – A Wisconsin state agency or local government.

Payer - A customer of the Biller's application that chooses to enter into a payment transaction.

Real-time - the quality that a process occurs synchronously and on-demand as opposed to a process occurring some time after the "demand", or request, when other conditions traditionally must be met, such as in "batch" processing.

Registration - the process by which a web user creates a "record" or collection of information that contains payment account data such as credit card or checking numbers.

Communication Protocols

Payer to Contractor
Communication of data between the Payer and the Contractor must be supported over https, strongly encrypted.

Biller to Contractor
The Contractor shall support the following file transfer protocols:

- sftp (secure ftp) via SSH;
- download via https on the administration site.

The Contractor shall support strongly-encrypted https for inbound and outbound communications.

The communication protocols shall apply whether the Contractor initiates contact with the Biller or vice versa. The protocol support must be configurable at the level of the Biller application. Some applications may require simultaneous support of multiple protocols.

The Contractor shall provide the following technical model for Internet Receipts:

2.1 Electronic Payment Gateway Technical Model

The Contractor shall provide a technical model where the Biller hosts the storefront pages and the Contractor hosts the payment page(s). The technical steps in this model are as follows:

1) Payer may be authenticated at the Biller's Website;
2) Payer enters appropriate information on Biller-hosted storefront pages in preparation for making a payment attempt;
3) Biller responds to Payer with a page containing session variables (e.g. invoice/order #, Biller ID, etc.) that may be transmitted by Payer to Contractor;
4) Payer requests the Contractor-hosted payment page(s), transmitting the session variables in the request. If this is the Payer's first payment attempt at the Contractor's Electronic Payments Website, the Payer may be required to provide registration data and select a User Name and password. This registration requirement must be configurable at the level of the Biller application.
5) The Payer shall also have the option to enter their User Name and password if they have registered previously;
6) Once the Payer's credit/debit card or bank account information has been entered, it shall be passed to the Nova Network for authorization or the bank RTN shall be validated;
7) Authorization/RTN results are received by the Contractor;
8) Payer is presented with a confirmation number or a transaction failure message. Contractor also presents access (links and/or buttons), as necessary, back to Biller's site. The access is provided by the EXIT button on the pages that directs the Payer to the Biller specified URL.
9) The Biller may elect to receive Real Time Payment Confirmation (RTPC) or Real Time Nonpayment Notification (RTNN) messages. If the payment is confirmed, an RTPC message shall be passed from the Contractor to the Biller's application or database in real-time. If the payment is not confirmed, a RTNN message shall be passed from the Contractor to the Biller's application or database in real-time. RTPC and RTNN messages will be sent via http or https in XML or URL encoded formats.

3.0 FUNCTIONAL AND TECHNICAL REQUIREMENTS FOR CREDIT/DEBIT CARD PAYMENTS RECEIVED THROUGH THE INTERNET

3.1 Credit/debit card payment pages

The Contractor shall provide a set of standard payment page templates for registration, authorization, payment scheduling and confirmation. The Biller shall be able to place customized text messages on the payment pages and shall be able to include the State's e-payment top banner on each page. Real-time communications shall be used for authentication, enrollment, authorization, payment scheduling and confirmation of each transaction. All payment screens must provide a URL link that shall allow the Payer to view the Biller's privacy policy. The Contractor-hosted credit/debit card payment pages shall accept data from the Biller's Web application. The Contractor shall allow the Biller to push up to 10 custom data elements to the Epayment Gateway System through Session Transfer Variables and XML. Session Transfer Variables shall be passed in an encrypted https POST method from the Biller Website to the Contractor's payment site. The Biller shall have the option of displaying all or none of the custom data elements on the payment pages.

The Contractor's credit/debit card payment pages shall collect the appropriate information from the Payer to create the authorization request to NOVA. The Biller may choose whether to invoke Address Verification Service (AVS) or Card Verification

Data (CVD), where data entry for zip code and the CVD digits shall appear on the page.

3.2 Payer authentication

The Biller shall have the option to pass any Payer authentication information collected by the Biller to the Contractor's Electronic Payment Gateway Service through a Session Transfer Variable or XML along with the payment amount and due date.

3.3 Initiate authorization request into the NOVA Network

After collecting the necessary payment information, an authorization request shall be sent to NOVA. Authorization request or failure with the appropriate failure code shall be received back from NOVA.

3.4 Real-time return of payment results to Biller Web application

The Contractor shall return the confirmation data below to the Biller. The Biller shall have the option to receive the authorization results through a real-time XML or URL-encoded file upon the event of the Payer clicking the confirm button for the payment. At a minimum, the following data shall be included in the file:

- Transaction confirmation id
- Biller product code
- Payment amount
- Convenience fee
- Payment effective date
- Amount due
- Due date
- Transaction mode (sent, return, refund)
- Any product parameters sent in the session transfer or collected from the Payer

3.5 Processing of special transactions

Billers shall be able to manually enter credit and debit card authorization requests for orders received by mail, telephone, or fax through an Administrative Site. Billers shall be responsible for authenticating those Payers who call, mail or fax, and for safe-storing the documentation to support the authorization of payments.

3.6 Payer confirmation screens/e-mail

The Payer shall be presented with detailed payment information to be verified before processing the payment. Only valid payments shall be presented for verification (the Bank RTN numbers have been successfully checked or credit/debit card numbers have been successfully authorized). The Payer may choose to receive a confirmation e-mail. Upon clicking the Confirm button, Payers shall be presented a printable confirmation page that shall include a confirmation number.

The Payer confirmation screens shall be customizable for each application to allow the display of product parameter data entered by the payer or passed in the session transfer. Any of the data elements interfaced under Section 3.1 may be included on the confirmation page. In addition, a customizable, 500-character instruction field shall be available near the top of the confirmation page. The field shall be customizable at the application level to include additional Payer instructions.

3.7 Response time

The Contractor shall release a payment success or failure response from its Web server within an average of 3 seconds from the time the payment authorization request is received by the Contractor to the time the response is released by the contractor (excluding delays caused by NOVA). In the event the Contractor's server complex is unable to successfully support this response time, the Contractor shall be responsible for re-engineering and upgrading its server complex to meet the standard.

3.8 Duplicate payments and payment statuses

The Contractor shall provide safeguards that prevent duplicate payments from occurring. Clicking the "Back" or "Submit" buttons inappropriately and other similar scenarios that might produce a duplicate payment shall be eliminated. The Contractor shall track all payments that are initiated but the authorization is denied, along with the reason code.

3.9 Deposit of settled transaction amount to Biller's bank account

For Visa, MasterCard and Discover transactions authorized no later than 1:00 a.m. C.T., the Contractor shall provide settlement to the Biller such that the proceeds from the charges and credits are deposited through the Automated Clearing House into the Biller's bank account that morning, if it is a business day, or the next business morning if it is a weekend or holiday.

3.10 Daily Remittance File

No later than 8:00 a.m. CT. the following business day, the Contractor shall make a remittance file available to the Biller. The remittance file shall contain a listing of the transactions that are settling to the Biller's bank account that day.

3.11 E-mail confirmation

If a Payer requested a confirmation via e-mail message or has entered an e-mail address as a registered Payer, the Contractor shall send a confirmation an e-mail message to the Payer within 2 minutes of the completion of the payment transaction. The email shall reference the name of the Biller application, the confirmation number and other product parameters as determined by the Biller. In addition, an e-mail message shall be sent to the Payer if the payment is subsequently returned for any reason.

3.11 Supported Internet Browsers

The Contractor's Electronic Receipting Service shall support and test against a range of Internet Browsers. At contract execution, the following browser versions are supported for both Windows and Macintosh Operating Systems:

- Microsoft Internet Explorer (version 5.0 or higher)
- Mozilla Firefox (version 1.0 or higher) (becoming available in late 2008)

On at least a semi-annual basis, the Contractor will test new browser versions of Internet Explorer and Mozilla Firefox. The Contractor will repair the application to the best of its ability, retest and migrate the modified code to the production platform. Upon the conclusion of this test, the Contractor shall notify the State Contract Administrator in the event it can not support any new versions of these browsers.

3.12 Compliance with credit/debit card operating rules

The Contractor shall, at its sole expense, perform the necessary maintenance and upgrades to ensure that the Electronic Payment Gateway Services are compliant with all credit/debit card operating rules.

4.0 FUNCTIONAL AND TECHNICAL REQUIREMENTS FOR AUTOMATED CLEARING HOUSE (ACH) PAYMENTS RECEIVED THROUGH THE INTERNET (E-CHECKS)

4.1 E-Check payment pages

The Contractor shall provide a set of standard payment page templates for registration, authorization, payment scheduling and confirmation. The Biller shall be able to place customized text messages on the payment pages and shall be able to include the State's e-payment top banner on each page. Real-time communications

shall be used for authentication, enrollment, authorization, payment scheduling and confirmation of each transaction. All payment screens must provide a URL link that shall allow the Payer to view the Biller's privacy policy. The Contractor-hosted credit/debit card payment pages shall accept data from the Biller's Web application. The Contractor shall allow the Biller to push up to 10 custom data elements to the Electronic Payment Gateway System through Session Transfer Variables and XML. Session Transfer Variables shall be passed in an encrypted https POST method from the Biller Website to the Contractor's payment site. The Biller shall have the option of displaying all or none of the custom data elements on the payment pages.

Once the required payment information has been entered, NACHA regulations require the Payer to accept the terms and conditions including authorization of the payment transaction via the ACH network. Once the terms and conditions are accepted, the Payer is taken to the "Payment Verification" page where they shall be required to confirm the payment information prior to processing.

The Payer also has the opportunity to cancel the payment prior to processing, lessening the risk of payment errors. If the Payer wishes to cancel the payment, he or she shall be able to do so by selecting the cancel payment button. If the Payer elects to cancel the payment, the Main Menu is displayed.

If a Payer attempts to make a payment and the RTN comes back invalid, the Payer is transferred to the "Make a Payment" page where an error message is displayed indicating that the correct bank account information must be entered.

4.2 Payment instructions

The Contractor must allow the following options for payment instructions (options shall be configurable at the product level):

- Accept the payment amount from the Biller-hosted web application;
- Allow the Payer to specify the amount and date of the payment;
- Allow the Payer to edit scheduled payments up until one business day before the settlement date;
- Allow the Payer to make one payment for multiple bills (assumes that when and if the payment amounts are passed to the Contractor from the Biller's website through a session variable, each will contain a unique identifier).

4.3 Non-recurring payments

The Contractor must support user authorization of online, non-recurring payments by requiring the authenticated Payer to accept the online Terms and Conditions. Authorization shall be displayed for the Payer during payment initiation and the Payer must authorize the transaction by clicking the Accept button before a payment can be processed.

4.4 Recurring payments

The Contractor must support user authorization of online recurring payments by requiring the authenticated Payer to accept the online Terms and Conditions. Authorization shall be displayed for the Payer during payment initiation and the Payer must authorize the transaction by clicking the Accept button before a payment can be processed.

4.5 Daily processing cut-off time and settlement

All ACH payments initiated by the Payer by 8:00 p.m. Central Time shall be credited to the Biller's bank account between 5:00 a.m. – 9:00 a.m. the next business morning and shall be considered collected funds at that time. Debit transactions shall be posted at the end of the business day and shall also affect the collected balance for that day. Any debits received throughout the day and credits received after the 9:00

a.m. window are reported to the Contractor's Information Reporting system for intra-day reporting and to wire transfer for daylight overdraft monitoring but post at end of day.

The Contractor must issue a warning message to the Payer if the Payer attempts to schedule a payment for a settlement date that is past the bill due date, or on weekends, federal, or state holidays. This assumes the Payer has elected to allow late payments.

4.6 ACH record formats

The Contractor must create ACH files in either the CCD format or the WEB Standard Entry Class (SEC) code, depending on the entity making the payment.

The Contractor shall provide the following additional file formats:

- NACHA PPD
- TEL

4.7 Bank Returns and ACH Rejects

The Contractor shall provide services to automatically redeposit, one time, all transactions returned for insufficient or uncollected funds. A report of all re-deposited transactions shall be available through the Contractor's information reporting services, data transmission, fax or mail. The transaction shall be posted to the Biller's settlement account only if it is returned a second time.

The Contractor shall help Billers handle returned items. ACH return items are matched on a combination of the trace number, receiving financial institution routing/transit number, credit versus debit trancode, dollar amount and account number. If one of these fields does not match, the Contractor's return item reporting shall provide the return as received and the originated information that differs from the return. Any unmatched returns shall be reviewed and settled to the Biller's settlement account. The Contractor shall provide a report of all unresolved returns.

To facilitate the matching process, originated transactions shall automatically be kept on file for ten days following the effective date.

4.8 Fraudulent transaction detection methods

The Payer shall be authenticated at the Contractor's Website. The Payer must enter their Payer Authenticator to proceed. If it does not match, they shall receive an error message. Once a Payer registers, on subsequent visits, the Payer Authentication sent during the session transfer is verified against the Payer Authentication saved in Payer's registration.

The Contractor shall provide the ability for the Biller to regularly transmit authentication data (i.e. User ID's and Passwords) for loading into the Electronic Payment Gateway System, so that Payer's may be automatically logged in.

4.9 Validating a Payer's account number structure and routing numbers

The Contractor shall verify the Payer's routing number at the time it is entered into the payment transaction. The routing numbers shall be verified by a mod 10 check and Thompson check. The Contractor shall also perform a calculation on the routing transit number to validate the check digit. As an optional feature, the account number can be scrubbed against a "bad check" database through eFunds ClickCheck or a similar product utilized by the Contractor.

4.10 Daily Remittance File

No later than 7:00 a.m. CT. the following business day, the Contractor shall make a remittance file available to the Biller in .csv and/or .xml format. The remittance file

shall contain a listing of the transactions that are settling to the Biller's bank account that day.

All returns shall be integrated into the remittance file. In addition, the Contractor shall use the NOC information to update the information for registered Payers.

4.11 NACHA Operating Rules

All Payer authentication, enrollment, authorization, payment scheduling and confirmation shall be done in conformance with NACHA operating rules. The Contractor shall also follow NACHA rules for consumer (WEB) and corporate (CCD) entries.

4.12 NACHA Security Audit

Upon request, the Contractor shall provide proof of a successful security audit.

5.0 FUNCTIONAL AND TECHNICAL REQUIREMENTS FOR IVR RECEIPTS

5.1 Technical model for Contractor-Hosted IVR with Authentication to Biller Database

In this technical model, the Contractor hosts the IVR and authenticates the Payer through a real-time read of the Biller's data base. The technical steps in this model are as follows:

1) The Payer calls the IVR hosted by the Contractor;
2) The Payer enters the authentication information into the IVR;
3) The Contractor sends a real-time request to the Biller's database to verify the Payer's authentication information;
4) If the Payer's authentication information does not match the Biller's database, the IVR responds with a message that the Payer is not eligible and who to contact;
5) It the Payer's authentication information does match the Biller's database, the IVR requests the necessary payment information;
6) The payment information provided by the Payer is read back to the Payer and they are provided a choice to make changes or confirm the payment;
7) If the Payer chooses to confirm the payment, the Contractor shall forward an authorization request through NOVA or shall verify the bank Routing Transit Number (RTN).
8) If the authorization/RTN verification fails, the Payer shall receive a prompt to re-enter the payment information or choose a different card/account.
9) If the authorization/RTN verification is successful, the Payer is provided with a confirmation number.
10) Authorization/RTN results are passed from the Contractor back to the Biller's database via XML or session transfer variables. The Biller's web application is updated in real-time with the results.

5.2 Toll-free number

The Contractor shall obtain and maintain a toll-free number for each IVR application.

6.0 ONLINE TRANSACTION WAREHOUSE FOR BILLERS AND PAYERS

The Contractor shall provide an Online Transaction Warehouse for access by Billers and Payers. Transaction data shall be available online for a period of at least 24 months from the settlement date.

6.1 Administrative Access by Billers

Billers shall be able to access the transaction warehouse online using a User ID and password. Billers shall be able to establish Security Officer profiles with different access rights. The Security Officer shall be able to create additional administrative users, enable or disable entitlements to administrative users, and reset passwords.

The information retained in the transaction warehouse shall include but is not limited to:

- All payment information collected – date processed, date settled, amount, payment status (confirmed, settled, returned), confirmation numbers;
- All payment type information passed from the Biller or collected from the Payer – payment type (unique identifier that recognizes Biller's payment), payment description, Payer account number (or other unique payment identifier that determines where the payment is posted), authorizations, confirmations, and rejections;
- ACH information including trace number and return reason code.

Returns and Notifications of Change
For returns, the Contractor shall provide support and reporting within the Administrative Website. The Contractor shall also provide support and reporting through fax, and mailed reports.

6.2 Payer Enrollment, Transaction and Account Management

Upon entering the Contractor's Payment Website for the first time, Payers are presented the option of registering in the system. A Payer who elects to register shall supply personal information such as name, e-mail address, and a shared secret. To allow Payers access to stored accounts and view Payment History on subsequent visits to the site, a user ID and password are selected during enrollment and entered the next time the Payer enters the payment site.

Registered Payers can use account management functionality that enables them to choose the account from which they shall make a payment. The system shall store multiple bank accounts and credit card accounts for each registered Payer. Registered Payers may also schedule recurring payments indicating the amount of payment to be made, the payment account from which payment is to be made, the frequency of the payment and when payments are to begin.

All Payers can schedule, edit, and cancel future-dated payments. Payers specify the settlement date on the "Make a Payment" page and edit or cancel payments up until the cutoff time for the day prior to settlement.

Unregistered Payers must input payment account information each time they make a payment. Payers who have not registered can access future dated payments only via the payment confirmation number.

Registered Payers shall also be able to view their payment history and gain access to vital payment information such as: the date payment initiated, date processed, account number from which payment was made, payment amount or return amount and payment confirmation number. Returned payments shall be indicated in the Payment history.

Registered Payers shall access their account information online. They shall be able to selected View Payment History which shall allow them to view and print a history of their transactions across all Biller applications. Payers who have not registered may access the history of the payment by entering their confirmation number. By viewing payment history, Payers can see payments that were returned.

7.0 ADMINISTRATIVE, RECONCILIATION AND REPORTING TOOLS

7.1 Standard Reports

A standard daily deposit report showing the transactions to be posted to the Biller's settlement account shall be available for viewing by Billers online via the administrative Website. Billers shall be able to sort at different levels.

The Contractor shall provide the following transaction and accounting reports and queries using secure Web-based methods:

- Transaction summary report showing the total transactions and dollar amount processed for the specified period;
- Transaction detail report listing each individual transaction, including the processing result;

7.2 Ad-hoc Reports

Billers shall be able to query the online transaction warehouse in real-time for both credit/debit card and E-Check transaction data by value or range of values for at least the data elements below. Query results shall be viewed online and may be exported to MS Excel.

- Transaction Date
- Payment Channel
- Payment Method
- Payment Status
- Decline Type
- Payment Amount
- Custom product parameters

7.3 Customer Support Inquiries

The Administrative Website shall provide a query screen for state agency customer support staff to view payer information and payment transaction details. The screen shall allow searching by User ID, Last Name, Company Name, and Confirmation Number. The payment transaction detail provided with the query results shall include the payment amount, payment date, and status. For e-checks, the detail shall also include the RTN, the last 4 digits of the account number, the ACH trace number, the ACH transaction code, the account type, and the account category. For credit/debit card payments, the query results shall provide the last four digits of the account number, the card expiration date, the card type and the authorization number.

7.4 Daily cash receipt remittance file

The Electronic Payment Gateway Service shall provide a daily file of all accepted transactions for reconciliation with the Biller's Web application and with the daily cash deposit. For each Biller application, the Contractor shall create a daily remittance file in ASCII and/or XML formats (at the option of the Biller). The daily Cash Receipt Remittance Files shall be available on both the Administrative Website and on the Contractor's secured FTP server no later than 7:00 a.m. Central Time. If the files are delayed, the Contractor shall notify the State no later than 7:00 a.m. Central Time. Included in the notification shall be an estimate of when the files will be available.

The file shall contain the following minimum data elements:

- Biller ID
- Confirmation Number

- Time the Confirmation Number was issued
- Payment Method (Credit Card/ICheck)
- Receipt Channel (IVR, WEB, POS)
- Payment Amount
- Card Type
- Authorization Code
- Payer Name
- Payer Address
- User Name

The file shall also contain a footer record that total the transaction counts and amounts by payment type and card type.

8.0 THE IMPLEMENTATION PROCESS

8.1 Implementation Questionnaire

The Contractor shall provide an Implementation Questionnaire for the set-up of each Biller application. The Implementation Questionnaire shall allow the Biller to select all of the set-up options necessary for implementation. The questionnaire shall be in either MS Word or MS Excel format.

8.2 Implementation Specialist

The Contractor shall provide the State with an Implementation Specialist who is familiar with the State's e-payment applications. The Implementation Specialist shall:

- Receive the Implementation Questionnaire.
- Within one business day, provide the State with the date that the application will be available for testing.
- Provide the Biller with a URL link to the test application upon completion of the set-up.
- Confirm the URL's used for RTPC and RTNN messages, Payers returning from the payment system, and email confirmation messages.
- Establish the administrative organizations at the time the initial set-up is complete.
- Answer any questions during set-up.
- Answer any questions regarding the set-up of production applications.
- Ensure that a mirror test-application is established the day the application is launched into production.

The State shall utilize the following email priority designations within the subject line, and the Implementation Specialist shall respond within the stated time period:

Low:	Response within 5 business days
Medium:	Response within 3 business hours (if submitted by 2:00 p.m. CT)
High:	Response within 1 business hour

8.3 Application Set-up

Each new e-payment application shall be available for testing within 7 business days of receipt of the completed Implementation Questionnaire.

8.4 Testing

The new e-payment application shall allow the State to process test transactions similar to the production application. The transactions shall be available within the transaction warehouse during testing. The daily remittance files, RTPC and RTNN messages shall also be functional during testing. The credit/debit card authorization process will not

be available for the application during testing. The Contractor shall provide the Biller with dummy account numbers to be used during testing.

8.5 Application Set-up Problems

9.0 BILLER AND DEVELOPER SUPPORT

9.1 Biller Training

The Contractor shall provide Web-based, online, and interactive instructions for Billers on how to use the administrative tools within the Contractor's Electronic Receipting system. Billers shall be able to begin training during the user-testing phase. The training shall include:

- An overview of the Contractor's Electronic Payment Gateway Service;
- How to use Administrative functionality (including generating reports and adding, editing, changing, and deleting transactions);
- How Payers use the Contractor's Electronic Payment Gateway Service (including making a one-time payment, making recurring payments and managing accounts);
- Problem resolution.

9.2 Developer Support

The Contractor shall provide online answers to frequently asked questions for access by State of Wisconsin developers during the set-up of new applications.

10.0 PAYER SUPPORT

10.1 Online Help Pages

The Contractor shall provide standard online HELP to Payers. A help page shall be accessible to all users, from any page within the system. It shall contain, at a minimum, the following:

- Explanations of the online payment process;
- Explanations of the purpose of each page;
- Explanations of all data elements the user is asked to provide;
- Frequently asked questions and answers to common Payer problems.

10.2 Payer Call Center

The Contractor shall provide call center support for Payers 24 hours a day, 7 days a week. The call center shall be available through a toll-free telephone number. The call center shall answer general Payer questions about the payment process, including but not limited to:

- Resetting passwords (after verification of shared-secret);
- Problems with user-id's;
- Payment confirmation.

The call center shall refer application-specific questions to a state agency contact provided by the Biller.

Call center services shall be available on a per-application basis.

11.0 INFRASTRUCTURE, AVAILABILITY AND DISASTER RECOVERY

11.1 Infrastructure

The Contractor's infrastructure solution shall include: Firewalls, Web Servers, Application Servers and Database Servers. The firewall shall provide security as users attempt to gain access to the Contractor's Electronic Payment Gateway Service. The Web server shall host the Internet content and provide it to users in HTML format. The application server shall host the State's Internet registration and payment applications and shall easily scale during peak Internet periods, allowing users to have uninterrupted access to the application database through dynamic Web pages. The database server shall provide for the storage of the system's registration and payment information.

The Contractor's Electronic Payment Gateway Service shall at all times be in compliance with the Payment Card Industry (PCI) Data Security Standard as updated by Visa/MasterCard.

11.2 System availability

Monthly Performance Standard
The Contractor's Electronic Receipting Service shall be available 99.50 percent of the time during the hours of 6:00 a.m. CT and 12:00 a.m. CT during any calendar month.

Daily Performance Standard
On the last two calendar days of each month, the Contractor's Electronic Receipting Service shall be available 99.90 percent of the time during the hours of 6:00 a.m. CT and 12:00 a.m. CT.

Outages caused by any of the following reasons shall be excluded for purposes of determining monthly or daily system availability:

- Periods of scheduled or emergency maintenance activities or a scheduled outage between the hours of 12:00 a.m. CT and 6:00 a.m. CT
- Problems with Content or the State's programming errors;
- Problems caused by systems administration, commands, or file transfer performed by the State's representatives;
- Interruptions in third party networks that prevent users for the Internet from accessing the State Website;
- Denial of service attacks, natural disasters, changes resulting from government, political, or other regulatory actions or court orders, strikes or labor disputes, acts of civil disobedience, acts of ware, acts against parties (including carriers and the Contractor's other vendors), and other force majeur events;
- Lack of availability or untimely response by the State to incidents that require the State's participation for problem source identification and/or resolution;
- The State's breach of its obligations under the Statement of Work.

11.3 Hot Back-up Facility

The Contractor shall maintain, at all times, a hot back-up facility that houses disaster recovery servers. Access control and physical security safeguards shall be implemented at both the production and back-up data centers.

The Contractor's Electronic Payment Gateway Service's server shall have both system and application data stored on mirrored EMC disk storage, allowing operations to continue in the event of a hard-disk failure. Data shall be replicated between the two data centers in order to maintain data synchronization in case of disaster recovery failover.

11.4 System scalability

The Contractor shall have the immediate capacity to process 50,000 Internet transactions and 50,000 IVR transactions per day for the Billers under this Agreement. The Contractor shall expand its capacity as necessary, to accommodate additional processing volumes under this Agreement.

11.5 Quality metrics

The Contractor shall provide a monthly report to the State on the following quality metrics:

- % availability and unplanned outage minutes for each Electronic Payment Gateway Service component:
  - Payment Website
  - Administrative Website
  - IVR
  - Real Time Payment Conformation
  - Real Time Eligibility Lookup
- Number of transactions processed by Biller and Payment Method.
- Average and maximum web response times by day.
- % of IVR responses within 1 second, 1-2 seconds, 2-3 seconds, > 3 seconds.

11.6 Contractor notification of system outages

The Contractor shall notify the Biller via e-mail within 30 minutes of the start of an outage or problem within any of the following Electronic Payment Gateway Service components:

- Payment Website
- Administrative Website
- IVR
- Real Time Payment Conformation
- Real Time Eligibility Lookup

Included within the email shall be:

- The component(s) affected.
- When the outage or problem started.
- The root cause of the outage or problem.
- An estimate of when the outage or problem will be resolved.

If the outage or problem lasts more than one hour, the Contractor shall provide hourly updates with any additional information.

The Contractor shall notify the Biller within 15 minutes of the resolution of an outage or problem within any of the components listed above.

11.7 Contractor troubleshooting of state-identified functional problems

The State may receive reports of system functional problems. The State shall send an email notification to the designated U.S. Bank Commercial Customer Service representative about the functional problem. The State shall include the following information about the functional problem within the email:

- The application reporting the problem
- Time the problem was first reported
- Description of the problem

- Payment screen where the problem occurred
- Payer Name
- Payment confirmation number if the payment was completed

Response Times
For functional problems that may be preventing Payers from successfully completing a payment, the Contractor shall respond to the State with an acknowledgement of the problem and an estimated time for resolution or the time for the next status update no later than 2 hours after the problem is first reported.

For other problems that do not affect Payers, the Contractor shall respond to the State with an acknowledgement of the problem and an estimated time for resolution no later than one business day after the problem is first reported.

11.8 Notification of system changes

The Contractor shall not introduce any changes in functionality or design to the product solution that are not backwards compatible with the Biller's Electronic Payment Gateway Service. The State shall be notified at least 60 days in advance of any such changes to the functionality or design of the product solution to allow for adequate lead time should the Biller opt to implement the change(s) to the Biller's Electronic Payment Gateway Service.

The Contractor shall provide an updated User Manual and technical specifications prior to the implementation of any change.

11.9 Disaster Recovery Plan

The Contractor shall be able to process all transactions within 72 hours of a disaster. All operating systems supporting the Contractor's Electronic Payment Gateway Service shall have backup and disaster recovery processes. All critical system components shall have a real-time, online backup. Multiple network paths shall connect the processors and the disk farm to enable rerouting of data.

The Contractor shall maintain a storage management strategy and a robust set of backup procedures. The strategy must efficiently utilize backup systems and capacities, as well as accommodate future growth.

The Contractor's disaster recovery plan shall include processes and procedures for:

- Nightly backups that are taken off site and secured at another secure location;
- Responsibilities of each member of the staff in case of system failure;
- Notification of key personnel in case of failure;
- Transfer and resumption of full operations/processing to the back-up data center to include disk monitoring, and off-site tape retention.

12.0 SECURITY

12.1 General

The Contractor shall secure the databases and servers that comprise the Electronic Receipting System. The Contractor shall provide adequate levels of physical security to protect against theft, tampering or damage. The Contractor shall protect the confidentiality, integrity and availability of the information collected, processed, stored and transmitted. Risks secured against shall include: interruption of computer services, unauthorized disclosure of information, loss of control over the system or physical damage or theft.

The Contractor shall provide personnel and access controls to protect against unauthorized access, including, but not limited to, password-protected access, access entitlement based on a "need to know" basis, separation of duties, employee background checks, and comprehensive security awareness training programs.

The Contractor shall provide adequate levels of network security to ensure the secure capture, storage and distribution of consumer financial information.

The Contractor shall notify the Biller in the event the security of their application has been compromised.

At the request and expense of the State, the Contractor shall submit to an external security audit.

12.2 Payer-to-Contractor

All payment pages shall use the https protocol under SSL 128-bit encryption. In transferring from the Biller application to the payment site, several data elements must be passed to create the customized Biller payment site. These variables shall be passed encrypted, in the https POST method. The Contractor shall supply the Biller with the encryption routine for the https POST routine. The Payer only requires a 128-bit browser to access the https payment site.

12.3 Contractor-to-Biller/Biller-to-Contractor

The Contractor shall support secured communications with the Biller. Data exchange shall comply with open, interoperable, secure standards to include transmission of data from and to the Biller using 1024-bit encryption (or higher) at the source and the support of a 128-bit secured socket layer (SSL) encryption. The Contractor's Electronic Receipting Service shall be able to accept a X.509 certificate and an LDAP bind through configurations at the iPlanet Web server.
When linking to a Biller site, the Contractor shall use an SSL certificate set to the 1024 bit encryption level. Whether a file or an HTML page is being delivered, its receipt is accomplished via the SSL protocol with 128-bit encryption protected by a site certificate from a credible Certificate Authority.

12.4 Failure monitoring/audit logs

The Contractor shall track all activity in logs to resolve disputes or reconstruct system events. Information recorded in the logs shall include transaction date and time, user identification or key identifier, Web transactions, IVR transactions, batch transactions, unique key data (enrollment ID, payment confirmation number) pertinent transaction data, success or failure indication of activity request.

The audit logs shall also track events of logins and logouts, any event where critical/secure data is viewed (payment information, personal information), any event that affects writing to the database (add, modify or delete), any event where information is passed to or from any external system, Java exceptions, database exceptions and other debugging information. Both the application and audit logs are meant for internal software debugging or tracking software or security incidents. It is not meant to be provided in any reporting to the Biller unless it is specifically requested.

12.5 Denial of service attacks

The Contractor shall employ a monitoring service that monitors the lines at all times. In the case of an attack, the Contractor shall work with the monitoring service to identify and trace the source of the problem so that the possibility of having an intruder breach the Electronic Receipting Service would be severely limited or eliminated completely.

If a perpetrator were actively engaged in attempts to "flood" the network, or disrupt connections between two computers, or disrupt service to a specific system or person, the Contractor's Computer Incident Response Team shall:

- Contain and/or eliminate the intruder via systemic means;
- Complete a Computer Incident Report;
- Analyze and upgrade the system to prevent the attack from reoccurring;
- Notify the proper authorities for legal action.

12.6 Spoofing

The Contractor shall utilize the following mechanisms to protect against spoofing:

1) Session Transfer Variables shall be encrypted as they are passed from the Biller's Website to the payment site, disallowing the modification of any of the data linked between the two sites;
2) Domain Name Services (DNS) is managed by the Internet Service Provider (ISP). The ISP provides a high level of security to protect these DNS servers. One of the first steps to prevent an attacker from gaining control over the traffic destined for the Biller's Website is to prevent the changing of DNS entries to re-direct traffic to a rogue Website.
3) Digital certificates for fully qualified domain names are obtained for the Contractor's Electronic Receipting Service. Only the domain owner can request certificates for the Contractor's registered domains. Certificates can only be issued to specific individuals at the Contractor. Once a certificate is obtained for the Website, the client browser checks the authenticity of the certificate against the domain. If the domain is "spoofed", the client shall receive a message on their browser indicating that the domain does not match the certificate.
4) Use of firewalls capable of detecting and preventing "spoofing" shall be deployed. The firewalls shall be capable of rejecting traffic that appears to originate from trusted zones but in reality is originated from untrusted sources. The firewalls shall also be capable of protecting against "TCP SYN" flooding attacks.

The Contractor shall utilize application monitoring to detect suspicious events and activity on the Biller's applications. These suspicious events and activities include repeated Shared Secret guessing attempts, repeated submission of malformed data to the application, or long-idle sessions. These suspicious activities shall be identified and captured for examination by security specialists. The Contractor's Electronic Payment Gateway Service shall have an automated response capability to freeze/block user accounts that appear to be the target of unauthorized access attempts. The freezing or blocking of a user account generally occurs when an authentication validation (Shared Secret) for the payment application fails three times in a row.

13.0 OTHER REQUIREMENTS

13.1 Web Standards

The Contractor shall comply with the State of Wisconsin guidelines for Web user interface design and presentation style within the constraints of the Contractor's product.

13.2 Section 508 Compliance

The Contractor's Electronic Payment Gateway Services must be 508 compliant.

13.3 Convenience Fees

The Contractor shall not charge any user, enrollment, convenience, surcharge or any other fees unless directed by the State. The State may elect to add a convenience or processing fee to the payment amount. For some applications, the State may require

that the convenience fee be shown as an additional and separate amount on the Payer's credit card or bank statement. This request must comply with all credit card associations' regulations.

13.4 Participation Agreements for Wisconsin Local Governments

The Contractor and the Local Government shall sign a Participation Agreement. The Participation Agreement shall not contain any terms that conflict with the Agreement. The initial Participation Agreements shall be for a term that ends no later than June 30, 2014. All Local Governments within the State of Wisconsin are eligible to sign the Participation Agreements.

13.5 Co-branding

Co-branding shall only be allowed with the prior consent of the State. For Local Governments, the Participation Agreement will indicate whether co-branding shall be allowed for the Contractor. Size and location are standard.

13.6 Subcontracting

At Contract start, the Contractor shall utilize Official Payments Corporation for the Department of Revenue credit/debit card tax payment application. The Contractor shall immediately notify the State in the event that any other subcontractors shall be utilized.

13.7 Privacy

Contractor shall not collect Social Security Numbers unless explicitly instructed by the Biller. Personal identifiers shall not be transmitted in the clear in open text anywhere along the transaction chain.

The Contractor shall not make any secondary commercial use of information/data collected from the Electronic Payment Gateway Service. The Contractor shall not share any information with third parties, subsidiaries or other entities.

Contractor shall provide their privacy and security policies to the State upon execution of the Agreement.

14.0 CONTRACTOR FEES

14.1 Billing/Monthly Invoice

The Contractor shall include the Electronic Payment Gateway Services fees within the monthly analysis statement of the associated settlement account.

14.2 Fee Schedule

Item	Measurement	Fee[1]
Internet Implementation and Set-up fees		
Per Biller Application	One-time	$950
IVR Implementation and Set-up fee		
Per implementation	One-time	$3,500

Application Reporting Fee Per Biller Application		
WEB w/o pre-registration	Monthly	$100
WEB with pre-registration	Monthly	$300
IVR	Monthly	$350
IVR and WEB	Monthly	$375

Payment Processing [1, 2]		
1 - 1,200,000	Per confirmation number generated	.24

> 1,200,000	Per confirmation number generated	.21
IVR Surcharge	Per minute	.08

Special Items		
Payer Call Center Support	Per Minute	$.95
Application-specific customization	Per hour	$150.00

1. Payment processing includes ACH Debit, Credit Card and Debit Card transactions initiated on the Internet and through Interactive Voice Response and then warehoused within the Contractor's Electronic Payment Gateway Service. Standard ACH and Merchant processing fees also apply.
2. The payment processing fee shall be calculated based on the annual confirmed transaction volume processed during the calendar year, January – December, and shall include all local government confirmed transaction volumes. The confirmed transaction volumes processed during the previous calendar year shall be the basis for the current calendar year fees.

15.0 Service Levels

Contract Section	Contract Language	Service Level Standard
Appendix 1, Section 7.4	The daily Cash Receipt Remittance Files shall be available on both the Administrative Website and on the Contractor's secured FTP server no later than 8:00 a.m. Central Time. If the files are delayed, the Contractor shall notify the State no later than 8:00 a.m. Central Time. Included in the notification shall be an estimate of when the files will be available.	The State has automated file transmission scripts that are run each day based on a 7:00 a.m. availability of the cash receipt remittance files. If the files are delayed without adequate notification, the State has to perform research to determine why the file transfers were not successful. The estimated out of pocket cost for this research is $300. Therefore, the Contractor shall reimburse the State $300 for each instance that the remittance files are not available by 8:00 a.m. Central Time and the Contractor has not notified the State of the delay by that time.
Appendix 1, Section 11.2	The Contractor's Electronic Receipting Service shall be available 99.50 percent of the time during the hours of 6:00 a.m. CT and 12:00 a.m. CT during any calendar month.	The Service Level Standard shall be calculated monthly. In order to meet the standard, outages cannot exceed 223 minutes in a calendar month. Prolonged outages that exceed 60 minutes in a calendar day shall be considered an "Out of Service Condition". An Out of Service Condition will occur if within the hours of 6:00 a.m. and 12:00 a.m. the combined outage time for the following Electronic Payment Gateway Services is 60 minutes or more: • Web Payment Channel • IVR Payment Channel • Real Time Payment Confirmations • Real Time Eligibility Lookups A system outage that affects multiple channels will only be counted once. U.S. Bank shall provide the State with an Out of Service Credit for each Out of Service Condition. The amount of the Out of Service Credit shall equal the Electronic Payment Gateway Service transaction processing fees for that day (does not include interchange, association and authorization fees paid to NOVA). All Out of Service Credits shall be credited to the State's Consolidated Analysis Statement during the month following the Out of Service Condition.
Appendix 1, Section	The Contractor shall notify the Biller via e-mail within 30	U.S. Bank shall notify the State via email within 30 minutes of the start of an

11.6	minutes of the start of an outage or functional problem within any of the following Electronic Payment Gateway Service components: • Payment Website • Administrative Website • IVR • Real Time Payment Conformation • Real Time Eligibility Lookup	unplanned outage within any of the following e-payment services: • Web Payment Channel • IVR Payment Channel • Real Time Payment Confirmations • Real-Time Eligibility Look-Ups If the State is not notified of an unplanned outage, agency staff will spend time troubleshooting their applications. The approximate service level failure cost incurred by an agency to perform this troubleshooting is $150/application. Therefore, for each failure to notify the State timely of an unplanned outage, U.S. Bank shall pay the State $450 as reimbursement for agency staff time spent troubleshooting the problem.
Appendix 1, Section 11.7	For functional problems that may be preventing Payers from successfully completing a payment, the Contractor shall respond to the State with an acknowledgement of the problem and an estimated time for resolution, or the time for the next status update, no later than 2 hours after the problem is first reported. For other problems that do not affect Payers, the Contractor shall respond to the State with an acknowledgement of the problem and an estimated time for resolution no later than one business day after the problem is first reported.	Functional problems that affect the Payer's ability to successfully complete a payment result in customer service calls to the state agency. The approximate service level failure cost incurred by an agency each day there is an e-payment functional problem affecting Payer's is $250. Therefore, for each e-payment application that experiences a functional problem affecting the Payer's ability to successfully complete a payment, the Contractor shall reimburse the State $250 per day, excluding the day the problem was reported, until the Contractor provides an estimated date/time of resolution.