Amendment No. 3
to
Contract No. NA130000088
for
Online Payment Transaction Services
between
JP Morgan Chase Bank
and the
City of Austin

1.0 The City hereby wishes to extend the above referenced contract for a period of 12-months. Effective November 20th, 2019, the term for the extension will be March 20th, 2020 to March 19th, 2021.

2.0 The total Contract amount is unchanged for the extension period. The total Contract authorization is recapped below:

Term	Contract Amount for the Item	Total Contract Amount
Initial Term: 03/20/2013 – 03/19/2016	$661,400.00	$661,400.00
Amendment No. 1: Option 1 – Extension 03/20/2016 – 03/19/2018	$903,650.00	$1,565,050.00
Amendment No. 2: Option 2 – Extension 03/20/2018 – 03/19/2020	$1,407,377.00	$2,972,427.00
Amendment No. 3: 12-month extension beginning 03/20/2020 – 03/19/2021	$0.00	$2,972,427.00

3.0 MBE/WBE goals were not established for this contract.

4.0 By signing this Amendment, the Contractor certifies that the Contractor and its principles are not currently suspended or debarred from doing business with the Federal Government, as indicated by the General Services Administration (GSA) List of Parties Excluded from Federal Procurement and Non-Procurement Programs, the State of Texas, or the City of Austin.

5.0 ALL OTHER TERMS AND CONDITIONS REMAIN THE SAME.

BY THE SIGNATURE(S) affixed below, this Amendment is hereby incorporated and made a part of the above-referenced contract.

Signature & Date:

Larnell Camus 11-26-19

Printed Name: Larnell Camus
Authorized Representative

JP Morgan Chase Bank
450 W. 33rd Street, 8th Floor
New York, NY 10001-2603

Signature & Date:

11/26/19

Daniel Dellemonache, Procurement Specialist III
City of Austin Purchasing Office

Amendment No. 2
to
Contract No. 5600 NA130000088
for
Online Payment Transaction Services
between
JP Morgan Chase Bank
and the
City of Austin

1.0 The City hereby exercises this extension option for the subject contract. This extension option will be March 20, 2018 through March 19, 2020. No options will remain.

2.0 The total contract amount is increased by $1,407,377.00 by this extension period. The total contract authorization is recapped below:

Action	Action Amount	Total Contract Amount
Initial Term: 03/20/2013 – 03/19/2016	$661,400.00	$661,400.00
Amendment No. 1: Option 1 – Extension 03/20/2016 – 03/19/2018	$903,650.00	$1,565,050.00
Amendment No. 2: Option 2 – Extension 03/20/2018 – 03/19/2020	$1,407,377.00	$2,972,427.00

3.0 MBE/WBE goals do not apply to this contract.

4.0 By signing this Amendment the Contractor certifies that the vendor and its principals are not currently suspended or debarred from doing business with the Federal Government, as indicated by the GSA List of Parties Excluded from Federal Procurement and Non-Procurement Programs, the State of Texas, or the City of Austin.

5.0 All other terms and conditions remain the same.

BY THE SIGNATURES affixed below, this amendment is hereby incorporated into and made a part of the above-referenced contract.

Sign/Date: Larnell Camos 4/25/18

Printed Name: Larnell Camos
Authorized Representative

JP Morgan Chase Bank
450 W 33rd Street 8th floor
New York, NY 10001-2603

Sign/Date:

Printed Name: James J. Howard
Authorized Representative

City of Austin
Purchasing Office
124 W. 8th Street, Ste. 310
Austin, Texas 78701

Amendment No. 1
to
Contract No. NA130000088
for
Online Payment Transaction Services
between
JP Morgan Chase Bank
and the
City of Austin

1.0 The City hereby exercises the extension option for the above-referenced contract. Effective March 20, 2016 term for the extension option will be March 20, 2016 to March 19, 2018 and there is one 24 month option remaining.

2.0 The total contract amount is increased by $903,650.00 for the extension option period. The total Contract authorization is recapped below:

Term	Action Amount	Total Contract Amount
Basic Term: 3/20/13 – 3/19/16	$661,400.00	$661,400.00
Amendment No. 1: Option 1 3/20/16– 3/19/18	$903,650.00	$1,565,050.00

3.0 MBE/WBE goals were not established for this contract.

4.0 By signing this Amendment the Contractor certifies that the Contractor and its principals are not currently suspended or debarred from doing business with the Federal Government, as indicated by the General Services Administration (GSA) List of Parties Excluded from Federal Procurement and Non-Procurement Programs, the State of Texas, or the City of Austin.

5.0 All other terms and conditions remain the unchanged.

BY THE SIGNATURES affixed below, this Amendment is hereby incorporated into and made a part of the above-referenced contract.

Signature & Date: Larrell Camus

Printed Name: Larrell Camus
Authorized Representative 3/14/16

JP Morgan Chase Bank.
450 W 33rd Street 8th floor
New York, NY 10001-2603

Signature & Date: Linell Goodin-Brown

Linell Goodin-Brownl, Contract Compliance Supervisor 3-22-16
City of Austin
Purchasing Office

Financial and Administrative Service Department
Purchasing Office
PO Box 1088, Austin, Texas, 78767

March 26, 2013
JPMorgan Chase Bank, NA
Ms. Larnell Camus
221 West 6th Street
Austin, TX 78701

Dear Ms. Camus:

The City of Austin has approved the execution of a contract with JPMorgan Chase Bank, NA for online payment transaction services.

Responsible Department:	Finance Department
Department Contact Person:	Diana Thomas
Department Contact Email:	diana.thomas@austintexas.gov 124 West Eighth St., Ste. 140, Austin, TX 78701
Department Contact Telephone:	(512) 974-1166
Project Name:	Online Payment Transaction Services
Contractor Name:	JPMorgan Chase Bank, NA
Contract Number:	NA130000088
Contract Period Amount:	NTE $661,400
Contract Period:	3/20/13 – 3/19/16
Extension Options:	Two (2) twenty-four (24) month extension options NTE 1) $903,650, and 2) $1,407,377. Total Contract NTE $2,972,427.
Requisition Number:	RQM 5600-12041600305
Agenda Item Number:	48
Council Approval Date:	12/6/12

A copy of the contract/purchase order will be forwarded by U.S. mail or email.

Thank you for your interest in doing business with the City of Austin. If you have any questions regarding this contract, please contact the person referenced under *Department Contact Person* above.

Sincerely,

David Kucko
Corporate Contract Administrator
(512) 974-3364

CC: Diana Thomas
Charles Purma

CONTRACT BETWEEN THE CITY OF AUSTIN ("City")
AND
J.P. Morgan Chase Bank, N.A. ("Contractor")
FOR
Online Payment Transaction Services

Contract # NA1300000088

The City accepts the Contractor's Offer (as referenced in Section 1.1.3 below) for the above requirement and enters into the following Contract.

This Contract is between J.P. Morgan Chase Bank, N.A. having offices at 221 West 6th Street, Austin, TX 78701 and the City, a home-rule municipality incorporated by the State of Texas, and is effective as of the date executed by the City ("Effective Date").

Capitalized terms used but not defined herein have the meanings given them in Solicitation Number BKH0152.

1.1 **This Contract is composed of the following documents:**

1.1.1 This Contract

1.1.2 The City's Solicitation, Request for Proposal (RFP), BKH0152 including all documents incorporated by reference

1.1.3 J.P. Morgan Chase Bank, N.A. Offer, dated June 11, 2012, including subsequent clarifications

1.1.4 Statement of Work, incorporated herein as Exhibit A

1.1.5 Pay Connexion Service Terms, incorporated herein as Exhibit B

1.1.6 Pay Connexion Standard Service Level Agreement, incorporated herein as Exhibit C

1.1.7 Fee Schedule, incorporated herein as Exhibit D

1.1.8 Pay Connexion Transaction Addendum to Select Merchant Payment Card Processing Agreement, incorporated herein as Exhibit E

1.1.9 Chase Onsite Card Payments, incorporated herein as Exhibit F

1.2 **Order of Precedence.** Any inconsistency or conflict in the Contract documents shall be resolved by giving precedence in the following order:

1.2.1 This Contract

1.2.2 The City's Solicitation as referenced in Section 1.1.2, including all documents incorporated by reference

1.2.3 The Contractor's Offer as referenced in Section 1.1.3, including subsequent clarifications

1.3 **Term of Contract.** The Contract will be in effect for an initial term of three (3) years and may be extended thereafter for up to two (2) twenty-four (24) month extension option(s), subject to the approval of the Contractor and the City Purchasing Officer or his designee. See the Term of Contract provision in Section 0400 for additional Contract requirements.

1.4 **Compensation.** The Contractor shall be paid a total Not-to-Exceed amount of $661,400 for the initial Contract term with two (2) twenty-four (24) month extension options in an amount of $903,650 and $1,407,377 respectively for a total estimated contract amount not to exceed $2,972,427. Payment shall be made upon successful completion of services or delivery of goods as outlined in each individual Delivery Order.

1.5 **Quantity of Work.** There is no guaranteed quantity of work for the period of the Contract and there are no minimum order quantities. Work will be on an as needed basis as specified by the City for each Delivery Order.

This Contract (including any Exhibits) constitutes the entire agreement of the parties regarding the subject matter of this Contract and supersedes all prior and contemporaneous agreements and understandings, whether written or oral, relating to such subject matter. This Contract may be altered, amended, or modified only by a written instrument signed by the duly authorized representatives of both parties.

In witness whereof, the City has caused a duly authorized representative to execute this Contract on the date set forth below.

J.P. Morgan Chase Bank, N.A.	CITY OF AUSTIN
Larnell Camus	Teresa Reddy
Printed Name of Authorized Person	Printed Name of Authorized Person
Larnell Camus	
Signature	Signature
Senior Banker	Corp Contract Compliance Manager
Title:	Title:
March 12, 2013	3/20/13
Date:	Date:

Exhibit A
Scope of Work

PROJECT SCOPE

Vendor's Responsibilities

The vendor will be responsible for all set-up, configuration and testing of the hosted system environment to meet the needs of the City's functional and technical requirements as described in this RFP.

The City intends to integrate department billing/sales systems with the hosted system using a phased approach. The vendor will be responsible for designing, constructing and testing all interfaces between individual department billing/sales systems and the hosted system. Upon the completion of each interface, the vendor will provide the City with documented dependencies between the systems along with specific guidelines for maintaining connectivity and up time.

The Vendor shall:

- Specify proposed demarcation of responsibilities between the City and the Vendor during system installation, testing, warranty, and maintenance
- Provide a detailed list of the necessary resources and expertise, complete with personnel job descriptions, which shall be required for the City to maintain the system once implemented

Specific deliverables are outlined in the Implementation section of this RFP.

City of Austin's Responsibilities

The City's personnel will be responsible for connecting the selected vendor to appropriate resources within the various City departments in order to implement the vendor solution. The City's project team will be comprised of a project manager, as well as technical and functional resources from the City's IT department, individual departments and financial services.

The City project manager will provide the following:

- Project prioritization and scheduling with the selected vendor's project manager.
- Access to office sites during normal business hours, based on approved criminal background investigation and formal badging process.
- Related documentation and/or access to appropriate technical resources from financial services and individual departments
- Issue identification, prioritization, communication to vendor support staff
- Scheduling and coordinating of regular project team meetings and work sessions as needed
- Office space for Vendor project management or technical resource staff, if needed.
- Facilities, including telephones, personal computer hookups, and access to copy and fax machines.

Facilities for all meetings, work sessions, and training classes, including any necessary audio-visual equipment.

Review and approval of milestones, deliverables, monthly status reports and invoices.

GENERAL REQUIREMENTS

Req #	Requirement Description	Required Response	Rating
G1	**Financial Stability:** The vendor must provide audited annual reports that demonstrate financial health of the organization.	Provide a minimum of two (2) most recent years of audited annual reports that evidence the financial health of the organization.	Pass/Fail
The JPMorgan Chase & Co. Annual Report for 2010 and 2011 can be accessed online via the following link: http://investor.shareholder.com/jpmorganchase/annual.cfm This link provides past and current JPMorgan Chase & Co. Annual Reports that can be accessed at any time by the City.			
G2	**Leadership Team:** The vendor must provide descriptions of senior management team.	Provide descriptions of the vendor's senior management team that detail their background and industry experience.	Must Have

Larnell Camus, the City's assigned Relationship Manager and Senior Banker, will be the primary contact for this RFP. We build relationships using a consultative, team approach and we assign a skilled team of experienced banking professionals dedicated to each relationship. In addition, J.P. Morgan's senior management takes an active role in working with our clients.

Relationship and Project Management Team

The City of Austin's designated Relationship Team is responsible for responding to your inquiries and requests for services, while attending to daily activities regarding the management of your accounts. The team is made up of professionals with a variety of expertise, providing individual answers by taking time to understand your business, listening carefully and proactively providing ideas to energize your business.

The City will also have an assigned Treasury Sales Manager, Beth Davidson. In addition, daily client service for your accounts will be handled by Valerie Hill, your dedicated Client Service Professional.

Upon award, a highly-qualified individual from each of the following teams will be assigned:

- Public Sector e-Payment Solutions Product Sales Specialists led by Jeremy Appel. The product sales specialists (PSS) will serve in a consultative capacity, facilitate the information exchange, analysis and requirements definition during the initial project phase, manage the City's overall relationship with the Pay Connexion solution and serve as an escalation point should one be needed.
- Public Sector Pay Connexion Implementation team, led by Patricia Carroll, who provides oversight and direction to dedicated Implementation Project Managers. Upon award and finalization of a Statement of Work, the City's Pay Connexion application(s) will be assigned within this unit. The Implementation Manager (IM) will serve as the project manager, technical subject matter expert ("customer engineer"), and primary customer support contact through the implementation and for the first 30 day post-launch.

We have included biographies of all Relationship Team members. Since the Implementation Project Manager is not assigned until a contract has been awarded, we have not included a biography for the Implementation Project Manager.

It is important to stress that the following team members are empowered to take whatever actions are needed to manage the City's relationship with J.P. Morgan.

Table 1 - Relationship Team Biographies

Relationship Manager	
Name, Title	Larnell Camus, Senior Vice President and Relationship Manager
Office Address	221 West 6th Street, Austin, TX 78701
Phone	512-479-2720
Fax	512-479-2814
E-mail	larnell.camus@chase.com

Larnell is the dedicated government banker for Chase in Hays, Travis and Williamson Counties. She is responsible for overseeing client relationships with the bank. Her primary responsibility is to provide solutions to meet client needs and is responsible for the overall satisfaction with the bank.

Larnell has been with Chase for 31 years and has experience in all aspects of commercial banking. Larnell has been on the board of the Austin Association of Financial Professionals for the last four years in different capacities.

In 2008, Larnell received the Chairman's Circle Award.

She is a graduate of Angelo State University with a degree in Business Administration.

Treasury Management Officer	
Name, Title	Beth Davidson, Assistance Vice President
Office Address	712 Main Street, 5th Floor, Houston, Texas 77002
Phone	713-216-8542
Fax	713-216-4048
E-mail	elizabeth.l.davidson@chase.com

Beth Davidson has worked for Chase for six years, beginning her career at Chase as a college intern. Beth joined the Treasury Services Sales team two years ago and previously worked in treasury operations and branch banking.

As a Treasury Representative in the Public Sector division of Chase, Beth is responsible for supporting treasury management relationships within the greater Houston for the government and not for profit clients.

Beth graduated from Miami University in 2006 with a Bachelor of Science in Business (Finance) and a Bachelor of Arts (Political Science).

Senior Client Service Professional	
Name, Title	Valerie Hill, Senior Client Service Professional
Office Address	221 West 6th Street, Austin, TX 78701
Phone	512-479-2029
Fax	512-479-2814
E-mail	valerie.j.hill@jpmorgan.com

Valerie Hill is a client service professional. She has 23 years of banking experience with Chase Bank. Valerie's experience includes positions in our Retail banking centers of customer service representative, licensed financial service representative, and financial sales representative. She has worked in the Austin middle market segment since 2006. As a senior client service professional, Valerie is dedicated to serving her clients in the Middle market sector. Her banking knowledge allows her to be very resourceful in finding resolution for complex issues and promptly responding to client request in the most efficient manner. Valerie has been awarded several Chase

Champion awards, which are recognition programs for those providing and exceeding client expectations. Valerie's clients value her as a dependable and important partner in assisting them achieve their financial goals.

Pay Connexion Implementation Project Manager Lead	
Name, Title	Patricia Carroll
Office Address	420 West Van Buren Street, Chicago, IL, 60606-3534
Phone Number	312-954-2703
Fax Number	312-954-2297
e-mail address	patricia.a.carroll@jpmchase.com

Patty has worked with Pay Connexion for 9 years and has 20 years of Onboarding, Operations, and Product Support experience. She also has significant implementation experience across industries including financial, government, utility, and insurance sectors. Patty is fully aware of the associated regulatory and customer experience issues that need to be addressed to deliver a successful solution on schedule.

Patty holds a Bachelor of Arts degree in History from St. Xavier University.

Pay Connexion Vice President, Product Sales Specialist	
Name, Title	Jeremy Appel
Office Address	Lafayette, CA
Phone Number	925-954-1963
e-mail address	jeremy.l.appel@jpmchase.com

Jeremy has worked on Pay Connexion for over six years in Product Management, Implementation and Sales functions and has more than fifteen years extensive Product Management, Marketing and Sales experience in other network, security and card related businesses. Jeremy holds a Bachelor of Arts degree in Sociology and Philosophy from University of Wisconsin Madison and MBA in Marketing and International Business from DePaul University's Kellstadt Graduate School of Business.

G3	**Risk Mitigation for Data Breach/Fraud:** The vendor must provide insurance, roles/responsibilities, policies and remediation procedures pertaining to data breach and fraud.	Describe how the system protects data from security breaches including how the impact to individual credit reports is controlled. Describe how notifications and costs are handled including the responsible party. Describe any security breaches to your system in the past five years.	Must Have

J.P. Morgan recognizes the paramount importance of the confidentiality, integrity, and availability of personal and e-payment related data. Pay Connexion e-payment solution utilizes industry leading security measures and is certified as being Payment Card Industry (PCI) compliant. The PCI-DSS certification confirms that we have taken the appropriate measures to ensure that we are protecting the City, the payer, and the card processing system from credit card fraud and other risks. These steps include requirements for security management, payment policies, data storage procedures, network architecture, software design, and other payment system measures.

Our data is housed in government grade robust, firewall-protected, and secure Oracle databases linked to Sun Solaris servers using SSL 1024-bit encryption for security. Geographically dispersed secure primary and back-up data centers help ensure application readiness and availability. J.P. Morgan systems will meet or exceed the City's security requirements.

With our Pay Connexion System, access to mainframe based information systems residing behind a firewall occurs through batch files securely transferred through the Internet.

Pay Connexion uses leading security measures when protecting users' credit card data. User information is both encrypted and transmitted over encrypted channels, regardless of the selected transportation method. Passwords are stored in a one-way hash. Sensitive credit card information, such as credit card number and expiration date, is encrypted using the triple data encryption standard (DES) algorithm.

Strict access control and physical security safeguards are implemented at both the primary and backup data centers to maintain a controlled, limited access environment for the areas supporting our payment solutions.

Payment accounts are always masked when displayed within our payments solution, with only the last 4 digits available for identification (e.g., XXXXXXXXXXXX1234).

To prevent unauthorized user access, we employ security measures to either the system or the data (compliance with PCI-DSS, CISP, SDP, etc.). J.P. Morgan's systems employ antivirus technology to protect integrity of both the User's and your organization's data. The Pay Connexion servers use the UNIX® operating system, which is not susceptible to viruses found in other operating systems. The virus protection is signature-based and is updated nightly, or more frequently as necessary. Additionally, a dedicated team of IT security professionals, called the Computer Security Incident Response Team (CSIRT), is constantly monitoring vendor or industry advisories for reported threats, vulnerabilities, or incidents. CSIRT is responsible for communicating and resolving issues around the clock.

Strict access control and physical security safeguards are implemented at both the primary and backup data centers to maintain a controlled, limited access environment for the areas supporting our Pay Connexion solutions.

Pay Connexion is listed with PCI-DSS as compliant, receiving a favorable rating from the assessor during the 2012 audit. Included in the PCI-DSS review is establishing and maintaining a secure network, protection of card holder information, data access and controls, and regular system and network monitoring.

In order to further reduce the potential for returned or fraudulent ACH/e-check payments, Pay Connexion offers the following validation checks:

- Mod-10 check on the bank RTN
- Verify bank RTN against a Database
- Account number validations
- Identification of Invalid Bank Accounts
- Disable payers from submitting new e-check Payments
- Notification of Change Updates.

J.P. Morgan will implement leading practices and industry standard measures to prevent, limit, and detect fraudulent transactions. Among those that we will implement are:

- When possible and relevant, we perform format validations, such as maximum/minimum character lengths and character types, such as currency, alpha-numeric, all numeric, etc.
- Our system checks dates to ensure dates are valid and they are actual valid dates in the future
- Our system validates phone number to ensure they are numbers and include the appropriate length
- Our system validates e-mail addresses to ensure they are consistent format (e.g., X@Y.Z)
- Duplicate payment check (An error message informs the payer the payment now being made may be a duplicate of a recent payment.
- Mod-10 check performed on the card number
- Card number check to verify that it is a valid length for the card type

	Card number check to verify that it starts with correct digits for card type Verification that there are no spaces in the card number and all characters are numeric An expiration date check to confirm that the card has not expired For Signature debit cards and pinless debit cards a card number check against a Bank Identification Number (BIN file) is performed to make sure that it is a valid card Billing address zip code format check During the credit card authorization process, the following validation is performed and the payment is either authorized successfully or declined: A payment amount check to make sure the payment does not exceed the available credit limit. A stolen card check to confirm the card has not been reported stolen A check to verify that the Issuer has not stopped all further payments on the card (placed by the card holder or the card issuer) Address Verification Service (AVS) Card Verification Data (CVD) Credit Card Authorization Attempt Limit (applies to the web only) By utilizing our Pay Connexion platform, all credit and debit card transactions are protected by the industry leading security technology and procedures.		
G4	**Customer References:** The vendor must provide customer references.	Provide a minimum of three (3) customer references ideally from related industries and project types.	Must Have

City of Grand Rapids, Michigan	
Contact Name	Al Mooney
Contact Title	City Treasurer/Treasury Director
Address	City of Grand Rapids Ste. 220 300 Monroe Ave. NW Grand Rapids MI 49503
Phone Number	(616) 456-3285
Email Address	amooney@grcity.us
Service Provided: City of Grand Rapids utilizes Pay Connexion Web and IVR in English and Spanish for multiple applications, including property taxes, water bills, parking violations, and miscellaneous receivables and uses On Site Card Payments with Convenience Fees for various payment types.	

City of Houston	
Contact Name	Jeffry Taylor
Contact Title	Utility Customer Service Supervisor
Address	4200 Leeland St Houston TX 77004
Phone Number	713-371-1114
Email Address	JEFFRY.TAYLOR@CITYOFHOUSTON.NET
The City of Houston uses PayConnexion for utilities and permits.	

City of White Plains, New York	
Contact Name	Nino Pennacchio
Contact Title	Comptroller
Address	255 Main Street White Plains, NY 10601
Phone Number	(914) 422-1397
Email Address	npennac@ci.white-plains.ny.us
Service Provided: City of White Plains utilizes Pay Connexion Web for multiple applications, including property taxes and utilities.	

G5	**Marketplace History:** The vendor must provide evidence of ongoing PCI-DSS (L1) certification.	The vendor shall provide evidence of experience in PCI-DSS (L1) industry with projects of similar size, scope, complexity.	Must Have

J.P. Morgan's e-Payment solution is certified by a qualified independent third party, Jefferson Wells, as being compliant with the Payment Card Industry Data Security Standards as a Level 1 processor, attests to the priority we give to the confidentiality, integrity and availability of our customers', and their customers', personal, account and e-Payment related data. The PCI-DSS certification confirms that we have taken the appropriate measures to ensure that we are protecting the City, the payer, and the card processing system from credit card fraud and other risks. These steps include requirements for security management, payment policies, data storage procedures, network architecture, software design, and other payment system measures.

Evidence of our PCI-DSS Compliance can be found at:

Visa: http://usa.visa.com/download/merchants/cisp-list-of-pcidss-compliant-service-providers.pdf
Search on "Pay Connexion".

MasterCard: http://www.mastercard.com/us/company/en/docs/SP_Post_List_2012.pdf
Search on "PayConnexion".

Pay Connexion has maintained its annual compliance status with no past penalties or infractions.

The Pay Connexion platform is being used today by other public and private sector clients to process over 19 million annual transactions totaling over $64 billion. There are hundreds of applications in production helping clients efficiently and securely collect payments for taxes, utilities, citations, permits, courts, insurance, financing, donations, invoices, advertising, child support, and more. This diverse range of applications, as well as the specific applications identified in the references section above illustrates the versatility of the Pay Connexion platform and J.P. Morgan's proven ability to support e-payment projects of comparable size, complexity and scope as that which the City has outlined.

G6	**Special Capabilities:** The vendor must provide descriptions of any knowledge, facilities or personnel that may add value to the scope of this RFP.	Describe any special knowledge, facilities or personnel relevant to this RFP.	Must Have

We believe that J.P. Morgan's size, strength, and market presence, coupled with our strong, proven technical solution and expertise, provide a best value solution to the City. We feel that our expertise as an authorized provider of e-Payment solution and merchant card services include:

- **Proven Processing Platform** - J.P. Morgan offers our commercially available service for processing ACH, debit card, and credit card payments through the Internet and telephone. The product is called Pay Connexion. Pay Connexion has been in existence for several years and has a proven record of system performance. It is an end-to-end solution and serves as a "hosted" system for processing card or e-check payments. It allows payers the choice to make payments through multiple channels, such as the Internet, automated phone, and call center administrative application. A shared database keeps a consolidated view of the payer, regardless of how they choose to make their payments. This same proven platform is being used today by other clients to process over 19 million annual transactions totaling over $64 billion.
- **Dominant in Merchant Processing** - The strength of our offering surpasses the offerings of third party providers because J.P. Morgan controls the entire lifecycle of an electronic payment – from the front end gathering of payment instructions from the payer via our Pay Connexion platform to settlement through our merchant processing company, Chase Paymentech. Chase Paymentech dominates the merchant acquiring market. In 2009, Chase Paymentech processed more than 18 billion transactions with a value exceeding $409.7 billion, including an estimated half of all global Internet transactions.
- **Cutting-Edge Payment Processing** – Our technology can help cut costs and increase productivity, and offers a payment processor that can provide solutions that evolve with the City's ever-changing needs.
- **Dedicated Customer Service** – The City will partner with a company whose professionals possess in-depth knowledge of the Payments industry, as well as an understanding of the City's unique business needs. Relationships are the foundation of our philosophy.
- **Sophisticated Reporting Capabilities** – The City will utilize an easy-to-use, flexible, and comprehensive reporting package that enables ongoing analysis and evaluation of transactions, settlements, chargebacks and other mission-critical information.
- **Competitive Pricing** – The City will minimize the costs involved in accepting payments. We have designed our solution to provide the City with the best value for your investment.

G7	**Research and Development:** The vendor must provide any capabilities that are relevant to maintaining competitive offerings.	Describe the size, staffing, resources and financial capabilities in place to maintain competitive offerings.	Must Have

Maintaining a competitive offering entails strategic planning as well as release of new and enhanced features over time. These functions fall under the dedicated Pay Connexion Product Management team's domain. This team sets the direction for internal dedicated Pay Connexion development and testing teams to execute. Other teams are dedicated to performing sales, implementation, client service, IT operations support, financial other related functions. All teams are staffed appropriately according to the strategic priority given to Pay Connexion as well as demand. Pay Connexion is well maintained with multiple releases per year. Pay Connexion's annual release schedule varies based on market and industry needs. Client feedback is crucial in our prioritization of the enhancements that are part of these releases. Feature Release notes regarding a particular release are normally distributed to clients 6-8 weeks prior to the release migration.

FUNCTIONAL REQUIREMENTS

The functional requirements describe product features and functionality requested by our end users. To ensure that a proposed solution is thoroughly represented, Vendors must respond to each requirement listed below.

"Importance Rating" indicates how critical the requirement is to achieving project objectives. The City's end users have assigned priorities to the functional requirements while our IT staff have assigned priorities to the technical requirement. The three "Importance Levels" are:

Must Have: These requirements may or may not be industry standards but are highly critical to the project. They must either be satisfied by the system's base functionality or the Vendor must offer an alternative to satisfy the base functional requirement.

Expected: These requirements are important to the end users of the system and generally describe features that are industry standards. The majority of these requirements need to be satisfied.

Desired: These requirements add value, but are not critical to our end users. These features are considered optional.

If there are responses that Vendors deem optimal to those suggested by the requirement description or response, please provide the alternate solution with a detailed explanation.

User Interface Requirements

Req #	Requirement Description	Required Response	Rating
F552	**Auto Data Field Population:** The system should auto populate repetitive data fields where pre-existing data has already been provided by the end user.	Explain how the system reduces repetitive data entry in application forms and/or tables (i.e. pre-fills, look-ups, etc.) for such things as names, addresses, etc.	Expected
Upon clicking the Pay Button, constituents will be passed via a session transfer to our secure J.P. Morgan-hosted Pay Connexion e-payment web site, where they will be able to execute the e-payment process. When the session transfer occurs, variable and/or static data parameters (e.g. utilities account number, service address, etc.) may be passed from the City's system to Pay Connexion in real-time. Pay Connexion also supports a batch			

interface for receiving data from the City, which is the Pay Connexion Pre-Registration File.

Delivering variable data in real-time via the batch Pre-Registration File or real time interfaces (e.g., session transfer and/or other Web Services API methods can prevent redundant data entry and may be useful, for example, if payers will have already logged into the City's website or otherwise searched there for their data.

If data is delivered in real-time during the session transfer:

- Pay Connexion can present to the payer the amount due that represents the unpaid balance, even if, for example, a partial payment received via a non-Pay Connexion payment channel had been posted earlier in the same day.
- Real-time data passed in the session transfer will override data delivered in batch via the pre-registration file.

If payers will have already logged into the City's web site before reaching the 'pay button', then Pay Connexion can support a single-sign-on user experience and pass variable data in the Web Services API session transfer. If not, then registered payers can log directly into the Pay Connexion Welcome Screen by use of a user ID and password combination. Which data elements are used as the User ID/Password is configurable by the City (e.g., account number / PIN). Upon successful payer log-in, variable data that was passed into Pay Connexion via the pre-registration file will be recalled. If the City uses our single-sign-on feature ("Auto Login"), then the Welcome Screen is bypassed altogether. If this feature is not utilized and the Welcome screen is presented, then some characteristics of the Welcome Screen itself will reflect City configuration selections.

Throughout the payment process, the Pay Connexion application offers assistance to payers through context-sensitive online help. The site is compliant with section 508 of the Americans with Disabilities Act.

If payers have been previously registered in Pay Connexion, their profile information (e.g., name, company, address, phone, email) is all pre-populated and there is no need for the information entered again redundantly. Similarly, if payers have previously saved payment card and/or bank accounts under their profile this information is retained for future use, however the sensitive account number is always masked when presented (e.g., XXXXXXXXXX1234) for security reasons.

Further, where the IVR payment channel supports City-registered payers who log in with all-numeric User ID/Passwords), City-defined parameter data (e.g., utility account number, amount due) may be passed into Pay Connexion via the Pre-Registration File and utilized during IVR payment sessions/calls.

F553	**Retain Input Data Values:** The system should retain previously entered application data as users navigate between related screens and/or modules.	Describe how the system retains data when data entry is suspended or interrupted by the user navigating away from the current focus.	Expected

Please see our response to *Req # F552* above.

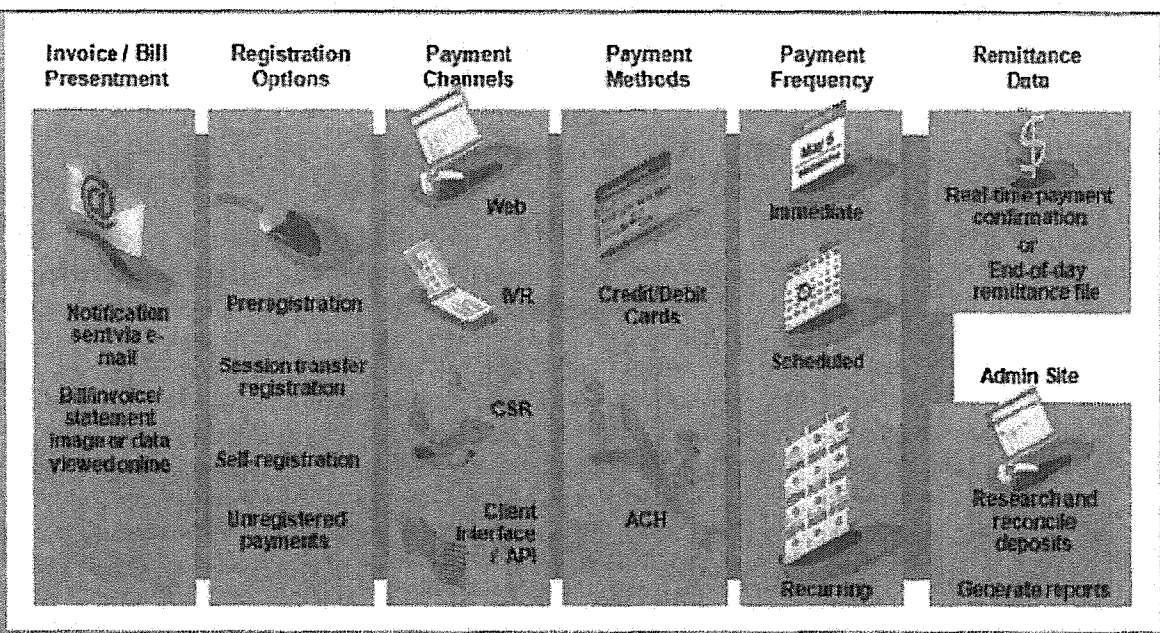
Additionally, note that information input into Pay Connexion via the Pre-Registration File and some of the Pay Connexion Web Services API Methods is retained in the Pay Connexion database and may be utilized in future sessions/calls without the need for redundant data entry. For example, a payer may see payer registration profile information (e.g., name, address, etc.) after choosing to view his/her profile. Information that is input into Pay Connexion via the real time Web channel session transfer from the City's systems (e.g., utility account number, amount due, due date) may be presented to the payer as soon has s/he is transferred into Pay Connexion. As payers and admin users advance from screen to screen in Pay Connexion, data that had been entered previously is preserved and presented as needed. Data that the payer adds (e.g., payment account-related information, specifically excluding the payment account number which is always presented masked as XXXXXXXX1234) is also preserved and presented as the payer/admin navigates through the various screens in the payment flow. Note, however, (whether the HTTPS Post or Web Services API Redirect session transfer type), is not retained because Pay Connexion recognizes that some data may be time-sensitive, and may no longer be accurate at the time the payer returns to Pay Connexion to complete a payment started previously.

Since the returning payer must initiate the session transfer from the City's site anew, the City has the ability to pass into Pay Connexion accurate and up-to-date data as needed for the application.			
F555	**Seamless User Experience:** The system should provide smooth transitions (continuity, without a loss of context) between department systems and the backend payment system.	Explain the flexibility contained in the system to support the development of smooth navigational integration to various application environments.	Expected
Please see our responses to *Req # F552 and #553* above. Pay Connexion supports a versatile and modularly expandable logical hierarchy in which differentiated payment flows may be supported as required by the City. Among variables that are supported in the Web session transfer or the IVR call and define the payer's experience are those that identify the specific payment flow into which the payer is passed in Pay Connexion. Different features of Pay Connexion are configurable at different levels of the Pay Connexion hierarchy: Biller Group, Biller, Product and Parameter. So for example, session transfer variables can route one payer's web session to the City's Parking Ticket "Product" under the Parking Enforcement "Biller" under a City-wide "Biller Group" and pass the parameters values of Amount Due = "$100.00" for Parking Ticket # = "12345" for License Plate State = "Texas" and License Plate Number = "ABC 123". Other "Products" may exist under the same Parking Enforcement "Biller" as defined by the City such as vehicle boot release fee, auto pound vehicle release fee, towing fee, monthly parking pass, etc., each of which would support City-defined parameters as applicable. A different payer who clicks on a different pay button may be routed into the City's utility bill payment flow under the Utility "biller", which could support an entirely different set of products and parameters as needed. It is by use of this logical hierarchy that each session for each application manages the context and navigational flow as needed. To give the user a seamless user experience and the confidence that they are making a payment to the City, rather than a third party, the payment web pages will include the City's web page logo/seal (160 pixels wide x 70 pixels high) in the upper left corner of the screen and banner (600 pixels wide x 70 pixels high) across the top of the screen to support the City's desired branding. The common look and feel of the payment site provides a consistent, seamless, and visually integrated user experience. Pay Connexion's Web and IVR channels may be configured for English only or English-Spanish. If a registered payer has defined a language preference, this language preference can be preserved through the web session transfer such that the preferred language is presented to the payer in Pay Connexion web channel. Pay Connexion can support City-defined labels for the User ID and Password, City-defined parameters, browser titles and more, which enables the use of the City's commonly used terminology. Additionally, Pay Connexion can support optional configurable static text boxes on various screens in the payment flow, which enable the City to provide informative messaging that is tailored to the application and context.			
F556	**Consistent City Branding:** The system may enable the City branded look and feel to be applied to appropriate screens.	Describe how the system can adopt a customized look and feel to match City branding and security guidelines.	Desired
Please see our responses to *Req # F552, #553 and #555* above. To give the user a seamless user experience and the confidence that they are making a payment to the City, rather than a third party, the payment web pages will include the City's web page logo/seal (160 pixels wide x 70 pixels high) in the upper left corner of the screen and banner (600 pixels wide x 70 pixels high) across the top of the screen to support the City's desired branding. The common look and feel of the payment site provides a consistent, seamless, and visually integrated user experience. To further support this seamless user experience, the payer may be returned to a URL of the City's choosing upon the completion or cancellation of a payment.			

Additionally, the City's graphics may be included at the header or footer of Pay Connexion generated emails (e.g., Payment Confirmation email) and the "from" email address may be defined by the City.			
F557	**Global Navigation:** The system may support consistent global user interface elements across disparate systems.	Describe how the system supports consistent global navigation across the entire end user experience.	Desired
Please see our responses to *Req # F552, #553, #555 and #556* above. Pay Connexion supports a consistent set of user interface elements across applications and payment channels (as applicable to each). For example, a variety of navigational buttons are available globally, including a Customer Service button, configurable Privacy Policy, context sensitive Help facility and Exit button (unless the City opts to suppress any of these). Depending on the City-defined application-specific configuration requirements, some applications might present a variety of menu options to registered payers, such as Make Payments, Manage Accounts (credit/debit card and bank accounts), Pending Payments, Statement History, Payment History, View/Update Profile, and Recurring Payments. Buttons are presented according to what is applicable for the payer in the given flow. For example, the Recurring Payments button might be presented in a utilities Make Payment flow but not in a parking ticket Make Payment flow. If the payer accessed Pay Connexion via the Manage Payments / Payment Inquiry flow rather than a Make Payment flow, the set of navigational buttons / menu options will exclude the ability to make a payment. City-defined application-specific configuration requirements will be defined during the Configuration Requirements Definition phase of implementation.			

Payment Requirements

Req #	Requirement Description	Required Response	Rating
F377	**Payment Type/Channel (Credit Card/Online):** The system must enable users to make online credit card payments for a product or service.	Describe how the system processes an online credit card payment.	Must Have
Pay Connexion will provide the City with the ability for your customers to process Credit and Debit Card payments via a website or interactive voice response (IVR). These payment channels are fully "hosted" by J.P. Morgan. Pay Connexion supports single payments through all payment channels, as well as recurring payments through its web payment channel. Pay Connexion also supports the real-time authorization and batch settlement of credit and debit card transactions. Additionally, Pay Connexion can support e-check payments that are processed as ACH debit transactions. The City can utilize Pay Connexion's Administrative web site for research, inquiries, and reporting. Pay Connexion provides industry-leading functionality, service, and support, yet can be quickly implemented in your environment to service both your customers and internal users. Pay Connexion provides a rich choice of configurable product options to meet your unique business needs. From hierarchically defined payment and processing rules across various lines of business, to unique variables that can be associated with each payment, we can provide a solution that addresses your unique needs. Pay Connexion has a full range of payment and presentment solutions, allowing the City to expand usage as your payment collection requirements change.			



Transaction Processing

In Step 1 shown in the following figure, the City has the option to pre-register users and to provide invoice data. Pre-registering users enables the "Auto Log-in" feature to further enhance the seamlessness of the user experience for payers that may have logged-in on the City's web site. It is common for property tax applications to support unregistered payments.

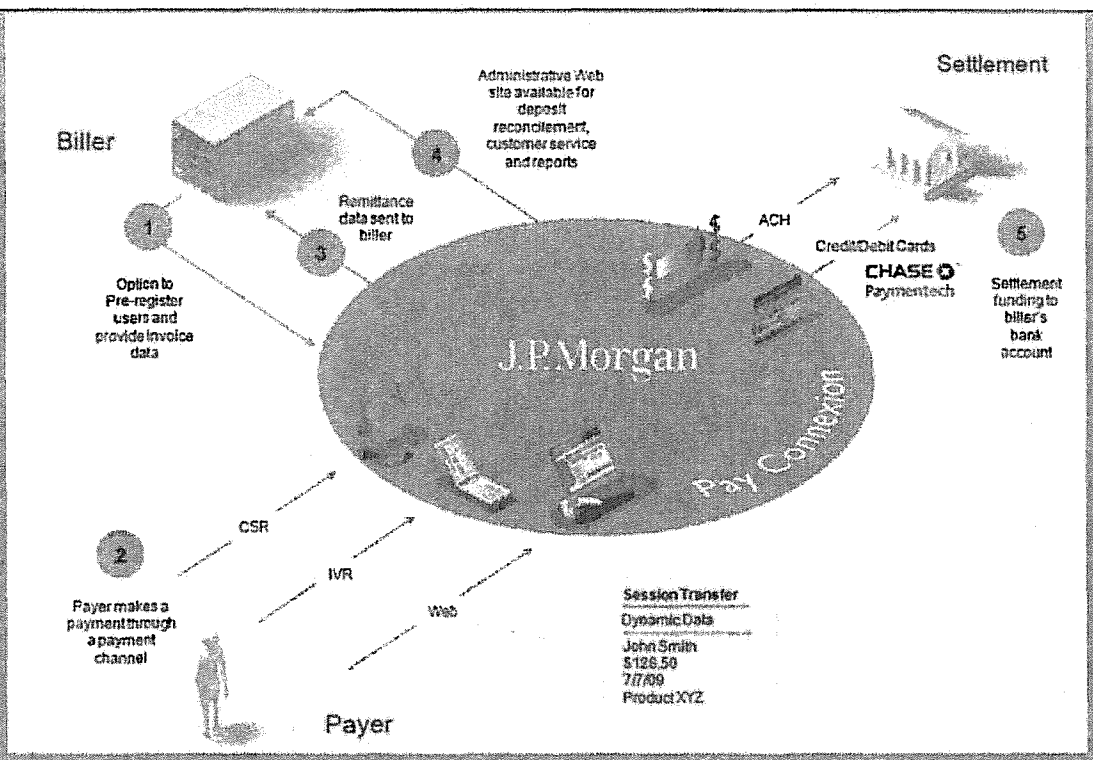
In Step 2, the payer makes a payment via credit, debit, or e-check.

Internet (Web) - Using a standard web browser, payers can make payments over the Internet. The session transfer registration gives the City the ability to register new payers and update profile information for existing payers. Executed in real-time when a payer clicks on a "Pay Button" on the City's website, constituents can access Pay Connexion to execute the payment process. The City's logo and banner graphics are displayed to seamlessly preserve the look and feel of the City's website. A shared secret value is used to authenticate unregistered payers when making payments by ACH.

In step 3, remittance data is sent to the City through a batch remittance file, a standard daily remittance file. An optional real time payment confirmation interface is also available.

In step 4, the City may use the Administrative website to research payment activity, generate reports, and/or download remittance information.

In step 5, settlement takes place. All credit and debit card payments are processed by J.P. Morgan Paymentech. Authorization takes place in real-time and are settled in batch. If supported in the City's configuration, all e-check payments are processed as ACH debit transactions by J.P. Morgan. All transactions are processed and settled in batch. Settlement funding is sent to the City's bank account held at J.P. Morgan.



Internet Payment Channel

Internet payers will access Pay Connexion's web payment channel via a session transfer that is executed in real-time when the payer clicks on a "pay button" on the City web site.

The Pay Connexion web payment channel can support both English and Spanish. The City's logo and banner graphics may be presented on all web channel web pages to provide a common look and feel with the City's web site and provide the payer confidence that he/she is using an official payment site. Additionally, the Chase logo may optionally be included on the web pages.

During implementation, J.P. Morgan provides the code that comprises the pay button. This code accounts for the City's unique parameters, as well as other application-specific configuration selections to be defined during implementation. The City will integrate this code into its existing web site. Pay Connexion supports HTTPS Post and Web Services API redirect session transfer interfaces as well as various feature-related Web Services API methods.

Upon clicking the "pay button", constituents will be passed via a session transfer to our secure J.P. Morgan - hosted Pay Connexion e-Payment web site, where they will be able to execute the e-Payment process. When the session transfer occurs, variable and/or static data parameters (e.g. ID number, Personal Access Code, etc.) may be passed from the City's system to Pay Connexion in real-time. Pay Connexion also supports a batch interface for receiving data from the City, which are the Pay Connexion Pre-Registration File as well as various feature-related Web Services API methods.

Delivering variable data in real-time via the session transfer may be useful, for example, if payers will have already logged into the City's website or otherwise searched there for their data. If data is delivered in real-time during the session transfer:

Pay Connexion can present to the payer the amount due that represents the unpaid balance, even if, for example, a partial payment received via a non-Pay Connexion payment channel had been posted earlier in

the same day.

Real-time data passed in the session transfer will override data delivered in batch via the pre-registration file.

If payers will have already logged into the City's web site before reaching the 'pay button', then Pay Connexion can support a single-sign-on user experience and pass variable data in an encrypted session transfer. If not, then registered payers can log directly into the Pay Connexion Welcome Screen by use of a user ID and password combination. Which data elements are used as the UID/PW is configurable by the City (e.g., account number / PIN). Upon successful payer log-in, variable data that was passed into Pay Connexion via the pre-registration file will be recalled. If the City uses our single-sign-on feature, then the Welcome Screen is bypassed altogether. If this feature is not utilized and the Welcome screen is presented, then some characteristics of the Welcome Screen itself will reflect City configuration selections.

Throughout the payment process, the Pay Connexion application offers assistance to payers through context-sensitive online help. The site is compliant with section 508 of the Americans with Disabilities Act.

Billers have several payment options which they can choose to offer to their clients: credit card, debit card, and e-check (ACH). Pay Connexion supports the real-time authorization and batch settlement of credit and debit card transactions. Additionally, Pay Connexion can support e-check payments that are processed as ACH debit transactions.

Credit, Debit, and Pinless Debit (ATM) Cards- Credit, signature debit, and pinless debit cards are accepted through all payment channels (Web, IVR, and Admin). Through our e-Payment application, we will accept all major credit and debit cards including Visa, MasterCard, Discover and American Express, however American Express is not available under the convenience fee model. Pay Connexion supports the use of ATM cards with NYCE, STAR, and PULSE logos. Card payments are authorized each time a new payment is initiated. Pay Connexion has unique intelligent functionality that recognizes a card number's BIN and can differentiate between a standard credit card and signature debit card. Payments are submitted using Chase Paymentech's merchant processing services. Thus, a separate merchant services agreement with Chase Paymentech Solutions is required with our recommended solution.

Transactions will be sent to Chase Paymentech's Authorization Transaction Database. During data validation and authorization, transactions are routed to the card issuing databases at the appropriate card organization (e.g., Visa, MasterCard). After authorization is complete, the settlement process begins in accordance with applicable rules, regulations and timelines. Customers will be notified if the card payment does not pass a series of validation and verification checks, including various card number validations, address verification service (AVS), card verification data (CVD) and authorization attempt limits, or if the card payment is not authorized by the merchant processor. Payment will only be confirmed when the validations and authorizations have occurred successfully. J.P. Morgan will retain credit card authorization logs and transaction records as required by applicable law and the rules, regulations, and operating procedures of the respective card organizations.

J.P. Morgan is responsible for capturing and validating the following information:

The payment amount is less than or equal to the Total Amount Due

The credit card or debit card number is checked and validated to meet with card organization rules

The proper credit card expiration date matches with the card issuing database

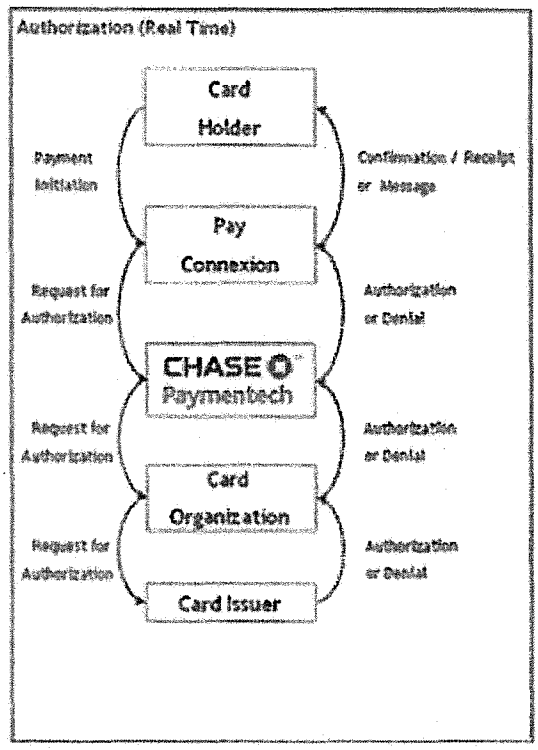
The name and address of card holder matches with the card issuing database

Telephone number exists and is a required field

The e-mail address is a required field and is a valid format

Pay Connexion supports the real-time authorization and batch settlement of credit card and debit card transactions. Pay Connexion processes credit/debit card transactions in coordination with the merchant processor (Chase Paymentech), the card organizations (e.g., associations/networks), and card issuers.

Processing:
Credit/Debit Cards



Each day's transactions, including adjustments, such as refunds and returns, are reflected in the daily remittance file. Additionally, the Payment Card Batch Report is available via the administrative site and is useful in reconciliation of card payments.

e-checks (ACH) - Pay Connexion can optionally support e-check payments that are processed as ACH debit transactions. ACH transactions are processed through a separate clearing network in batch process, per NACHA guidelines. e-checks/ACH debits are a popular, low-cost electronic payment alternative to payment cards. Pay Connexion supports the acceptance of all consumer and business e-check payments, processed through ACH.

All e-check/ACH payments are made in compliance with NACHA and applicable regulatory requirements. Among the NACHA requirements that Pay Connexion supports is that the Biller employ commercially reasonable measures for authorization and authentication to minimize the potential for fraud. Pay Connexion assists the Biller in meeting these requirements through the use of a shared secret, called 'Payer ID', that is determined during implementation. This value can be passed to Pay Connexion in the session transfer, or via a pre-registration file, if used.

Routing Number: 021000021

Account Number: XXXXXXXXXXXXX3456

Account Type: Checking

Account Category: Business

E-mail Address: tim.m.temp@jpmchase.com

Send me an email confirmation: ☐

Language Preference: English

Enter Password*: ••••••••••

Terms And Conditions

PLEASE READ AND APPROVE THE FOLLOWING AUTHORIZATION

By clicking "I Accept", I authorize the payee to electronically debit my bank account for the amount(s) and date set forth above. This authorization is valid for this transaction only.

If a convenience fee is added to the transaction, I understand that the convenience fee displayed will be included in the total payment amount.

In the event that a payment is returned for insufficient funds, I authorize the payee to electronically debit my bank account for the original amount of the transaction, as well as a returned item fee, up to the maximum amount allowed by law.

PLEASE PRINT A COPY OF THIS AUTHORIZATION FOR YOUR RECORDS

I accept the Terms and Conditions*: ☐

Confirm Cancel

In order to further reduce the potential for returned or fraudulent ACH/e-check payments, Pay Connexion offers the following validation checks:

- Mod-10 check on the bank RTN
- Verify bank RTN against a Database
- Account number validations
- Identification of Invalid Bank Accounts
- Disable payers from submitting new e-check Payments
- Notification of Change Updates.

J.P. Morgan will originate ACH debits on behalf of the City and settle ACH payments to a City DDA at J.P. Morgan.

Regardless of the payment method used, if a payment transaction is authorized, a confirmation page is presented to the payer. The confirmation page may be printed for a hard-copy receipt. The payer also has the option of providing an email address (unless required by the City). If provided, the payer may have the payment confirmation sent via email. A unique Pay Connexion confirmation number is assigned to every payment made and provided to the customer upon payment submission. With a confirmation number, a payer will be able to view the payment initiation date, the date a payment was processed, the account number from which the payment was made, the payment amount, and the payment confirmation number. Once a payment is submitted, the customer can immediately "recheck" the status of their payment. The payment can be viewed on the payment site immediately following the payment.

Settlement processing and timing is in accordance with the standard timeframes as indicated below for supported payment vehicles.

If supported in the City's configuration, all e-check payments are processed as ACH debit transactions by J.P. Morgan. All transactions are processed and settled in batch.

All credit and debit card payments are processed by Chase Paymentech Solutions. Authorization takes place in real-time and are settled in batch.

If ACH/e-check e-payments are supported in the City's configuration, these transactions will be processed as ACH debits originated by J.P. Morgan on behalf of the City through J.P. Morgan's ACH processing platforms. All ACH/e-check payments made each business day before 9:00 PM ET will be processed in a batch and presented for processing. The Pay Connexion system will debit funds from the customer's account via ACH and credit the City's DDA held at J.P. Morgan. Funds will settle on the next business day (excluding weekends and Federal Reserve holidays) to the City's DDA at J.P. Morgan.

Payment Settlement for Card transactions varies depending upon which platform the client is on. There are two platforms: Global and North American.

Below is the typical settlement timing for e-payment transactions; however, the City has flexibility to choose different cut-off times.

Table 2 - Cut-Off Times

	Credit/Debit Card Transactions Authorized Through Chase Paymentech – Global Platform
	Day Paid via ACH for Transactions
Card Transactions (Day of Batch Closed)	Visa, MasterCard & Discover

Monday	Tuesday	Monday 8 pm EST	Wednesday
Tuesday	Wednesday	Tuesday 8 pm EST	Thursday
Wednesday	Thursday	Wednesday 8 pm EST	Friday
Thursday	Friday	Thursday 8 pm EST	Monday
Friday	Monday	Friday 8 pm EST	Tuesday
Saturday	Tuesday	Saturday 8 pm EST	Wednesday
Sunday	Tuesday	Sunday 8 pm EST	Wednesday
		Credit/Debit Card Transactions Authorized Through Chase Paymentech – North American Platform	
Payment Completed	**ACH/ e-check Payment (9 pm ET Cut-Off)**	**Card Transactions (Day of Batch Closed)**	**Day Paid via ACH for Transactions**
			Visa, MasterCard & Discover
Monday	Tuesday	Tuesday 5 am EST	Wednesday
Tuesday	Wednesday	Wednesday 5 am EST	Thursday
Wednesday	Thursday	Thursday 5 am EST	Friday
Thursday	Friday	Friday 5 am EST	Monday
Friday	Monday	Saturday 5 am EST	Tuesday
Saturday	Tuesday	Sunday 5 am EST	Wednesday
Sunday	Tuesday	Monday 5 am EST	Wednesday

F385	**Payment Type (Credit Card):** The system must support credit card payments for the following types: Visa, MasterCard, Discover, and American Express.	Describe the credit card vendors that the system supports. What capabilities does the system have (if any) to add additional payment card types presently or in the future?	Must Have

During the Configuration Requirements Definition phase of implementation the City may choose which card types will be supported from those that Pay Connexion accepts. Credit, signature debit, and pinless debit cards are accepted through all payment channels. Through our e-Payment application, we will accept all major credit and debit cards including Visa, MasterCard, Discover and American Express, however American Express is not available under the convenience fee model. Pay Connexion supports the use of ATM cards with NYCE, STAR, and PULSE logos. If Pay Connexion is modified to accept additional cards, these may be made available to the City.

F375	**Transaction Fee Administration:** The system must provide a flexible model for configuring and administering the payment of transaction fees.	Describe the capabilities the system provides for: Assigning transaction fee types (percentage or fixed fee) to specific types of transactions (e.g., by transaction type, merchant ID or department system) Assigning the transaction fee payer (e.g., citizen, department, central fund, hybrid) Debiting appropriate accounts for fees due at set intervals. (Expected) Describe how other fees (i.e. interchange, merchant processor or bank) are assigned and collected (e.g., to citizen, initiating department).	Must Have

Pay Connexion provides the flexibility to be funded by any of the following models:

No Cost Convenience Fee Model - Pay Connexion is able to support many convenience fee structures, such as percentage, tiered, or flat fees. Convenience fees may differ by payment method and are configured at the "biller-level" in the Pay Connexion logical hierarchy. With the No Cost Convenience Fee Model, a convenience fee is passed on to the payer during the payment transaction and the City pays no fees. Upon acceptance of a convenience fee, the convenience fee is displayed to the payer separately from the payment amount. The convenience fee is charged to the payer at the time of payment. The payer will see two transactions listed on their credit card, debit card, or checking account statement. J.P. Morgan collects the convenience fee from the payer and pays all expenses associated with the transaction, including interchange, dues, assessments, and merchant processing fees. In this model, the City does not pay implementation, hosting, or per transaction fees.

City-Funded Model - Through a City Funded fee model, fees for the application are passed on to the City, and use of Pay Connexion is free to the payer. Typical City Funded costs include setup (implementation), monthly hosting, and per transaction fees paid by your organization for the application. Some specific fee levels are configuration-driven. Additionally, the City pays the related credit card discount fees/interchange and merchant processing fees. Under this model, the card processing fees are debited from the City's designated DDA for each Merchant ID as defined during the Configuration Requirements Definition phase of Implementation.

Hybrid Model – Pay Connexion is able to support many convenience fee structures, such as percentage,

tiered, or flat fees. Convenience fees may differ by payment method and are configured at the "biller-level" in the Pay Connexion logical hierarchy. The City can designate a convenience fee during the Configuration Requirements Definition phase of Implementation which the City will collect. Upon acceptance of a convenience fee, the convenience fee is displayed to the payer separately from the payment amount. The convenience fee is charged to the payer at the time of payment. The payer will see two transactions listed on their credit card, debit card, or checking account statement. Typical City Funded costs include setup (implementation), monthly hosting, and per transaction fees paid by your organization for the application. Some specific fee levels are configuration-driven. Additionally, the City pays the related credit card discount fees/interchange and merchant processing fees. Under this model, the card processing fees are debited from the City's designated DDA for each Merchant ID as defined during the Configuration Requirements Definition phase of Implementation. Under this model, a portion of the solution may be funded by the payer in the form of a convenience fee and a portion is funded by the City.

F403	**Transaction Delivery Timeframe:** The system should batch transactions at least daily.	(Credit Cards) Describe the timeframe that the system holds credit card transactions before they are sent to the merchant processor. (ACH Transactions) Describe the timeframe that the system holds credit ACH transactions before they are sent to the payment gateway.	Expected

Please see our response to *Req #F377*.

Pay Connexion supports the real-time authorization and batch settlement of credit and debit card transactions.

Electronic check payments are processed as ACH debit transactions that are processed through a separate clearing network in batch process, per NACHA guidelines. All transactions are processed and settled in batch.

Since the card and ACH payments are processed through different networks, and Pay Connexion can utilize either of two Chase Paymentech merchant processing platforms, there is a variety of options for card and ACH batch close times. During the Configuration Requirements Definition phase of implementation the optimal batch close times will be determined for each application.

F531	**Duplicate Transaction Prevention:** The system should provide controls to prevent duplicate transactions.	Describe how the system prevents the use of the same unique transaction identification number.	Expected

Pay Connexion supports logic to help ensure that duplicate payments do not occur. The logic helps ensure that the payment a payer is making now does not duplicate a previously made payment. The exact logic utilized in any given payment is a function of the application configuration specifics as well as the session specifics and other factors. In the event that the current payment seems to duplicate a prior payment, the payer is given a warning that the current payment may be a duplicate is presented with information identifying the prior payment and is given the option to cancel or continue with the current payment.

Moreover, Pay Connexion generates a unique payment confirmation number for each payment transaction. This is the case for single payments, whether immediate or future-dated ("warehoused"), when non-payment initiation actions are executed (e.g., a payment is edited or refunded), and when instances of recurring payments occur. Recurring payment authorizations/instructions result in a unique recurring payment reference number.

F526	**Transaction Validation (ACH/EFT):** The system should validate the routing number and account number during ACH/EFT	Describe the process the system uses to validate ACH/EFT transactions.	Expected

	transaction process.		
Please see our response to *Req #377*.			
F388	**Payment Refund (Credit Card):** The system should provide refunds of a transaction or portion of a transaction for a product or service.	Describe how the system provides payment refunds for credit card transactions.	Expected
Authorized City personnel will have access to an administrative website where they can research transactions and initiate a refund if appropriate (whether a payer has made an erroneous, duplicate, or incorrect payment). After recalling the payment, they select the Refund Payment button. This button, which is available immediately for credit card payments, and after 10 days for ACH/e-check payments (to minimize the risk of a return of a transaction that was refunded), takes the administrative user to the Refund Payment Screen. Administrative users are able to post partial amount refunds or refunds for the entire original payment amount. Administrative users cannot issue a refund for more than the total original payment amount (including the convenience fee, if applicable). J.P. Morgan will automatically process the refund and credit the payer through the account from which the original payment was initiated. Following a partial refund, subsequent refunds may be initiated up to the original payment amount. In the event of a payment refund, the convenience fee may be refunded.			
F392	**Voiding a Transaction (Credit Card)**: The system should allow an authorized user to void a transaction within the same day the original posting is made prior to batch processing.	Describe how to void a transaction in the system including any controls to limit this activity (e.g., transactions can only be voided on the date the transaction was originally posted).	Expected
Voids may be executed by the City's authorized personnel via the Pay Connexion administrative site with supervisory approval.			
F381	**Payment Chargeback (Credit Card):** The system should enable the resolution of a payment chargeback.	Describe how the system processes a payment chargeback.	Expected
The Chase Paymentech Chargeback Department will work with the City to evaluate every disputed charge. If Chase Paymentech is unable to remedy the chargeback, we send it to you with all supporting documentation. You may then research the transaction for a possible remedy. Included in each chargeback package is a merchant recourse form, which outlines the nature of the chargeback and the information required to reverse it. Chase Paymentech's chargeback support will ensure that this impact is minimized. Chargeback retrievals are a request for information from the issuing bank. They are typically initiated upon a cardholder's request. If the cardholder does not recognize a charge on their billing statement, they may contact their bank and request further information. This is done as a Chargeback Retrieval Request. Chase Paymentech receives retrieval requests electronically as part of their daily incoming chargeback files. They are matched against the Order History Database and a facsimile draft is produced which is either mailed or imaged to the initiating issuing bank. Chargeback retrieval requests are also delivered to the merchant in order to obtain the required proof of the transaction. The printed proof of the transaction is then attached to the document and forwarded to the Issuer. According to Visa and MasterCard Operating Regulations, an acquirer (i.e., Chase Paymentech) has 30 calendar days from the date received to fulfill a chargeback retrieval request (also referred to as a "request for copy"). Merchants are given until day 16 of the 30-day lifecycle to fulfill ticket retrieval requests. If a request is unfulfilled as of day 14, Chase Paymentech will send a second request via fax, provided that the merchant is set up for fax			

delivery of their retrieval request notifications. Generally, if a retrieval request is not fulfilled (i.e., copy of receipt is not presented), the retrieval becomes a chargeback. Facsimile and scanned images are acceptable means of producing the requested drafts. Chase Paymentech ensures that operating procedures for exception processing, including retrievals and chargebacks, minimize Biller impact while addressing cardholder issues. Chase Paymentech's processing rules are written to generate a retrieval or chargeback response without City involvement if the required information is accessible by Chase Paymentech. Customer support will be handled by the Operations Practice Management (OPM) team. OPM is available to support the City 24/7/365 via a toll free phone number. OPM will work with Chase Paymentech to designate a Chargeback Analyst to assist with your account. Your designated Chargeback Analyst will be the single point of contact for all chargeback issues (with additional assistance from your Account Executive). Your Chargeback Analyst will review every chargeback for proper documentation and adherence to the payment brands' rules and regulations. All items are addressed and processed within the required time frames to ensure that your re-presentment rights are fully preserved.			
F380	**Payment Type (ACH):** The system should process Automated Clearing House (ACH) payments.	Describe how the system supports the processing of ACH payment. If the system does not support this payment type then provide a detailed description of how the system integrates with other vendor systems that do provide this capability.	Expected
Please see our response to *Req #377*.			
F376	**Payment Type (PINless Debit Card):** The system should process PINless debit card payments for a product or service.	Describe how the system supports the processing of PINless debit cards for payment. If the system does not support this payment type then provide a detailed description of how the system integrates with other vendor systems that do provide this capability.	Expected
Please see our response to Req #377.			
F378	**Payment Channel (Mobile Device):** The system should enable customers to pay for products and services from a mobile device.	Describe how the system supports the processing of payments from a mobile device. If the system does not support this payment channel then provide a detailed description of how the system integrates with other vendor systems that do provide this capability.	Expected
Pay Connexion supports a mobile payment channel. On an application-specific basis, City-registered payers may enroll via the web channel for mobile payments. To establish a relationship of recognition between the Pay Connexion, the payer and his/her mobile device, the process of enabling payers that are pre-registered by the City to enroll for mobile payments includes the following steps: 1. Payer provides the mobile text number on the Pay Connexion 2. Payer receives Activation Code text on his/her mobile device			

3. Payer provides Activation Code in Pay Connexion to complete enrollment
4. Payer views Mobile Text Enrollment Confirmation on Pay Connexion
5. Payer receives Enrollment Confirmation text
6. Payer receives Enrollment Confirmation email

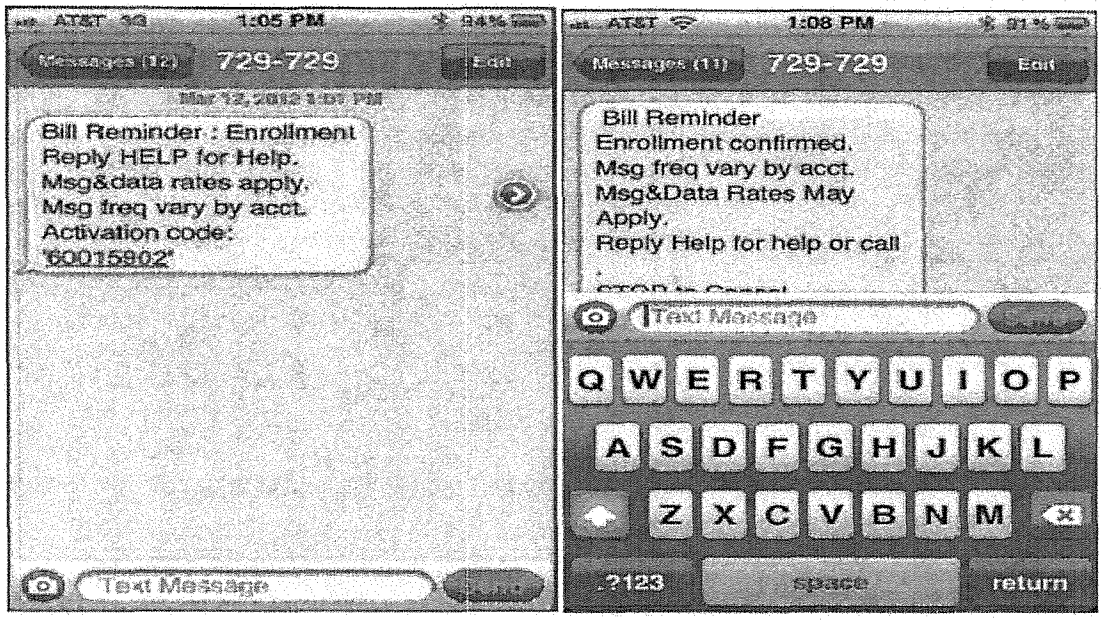


Figure 5. Sample Enrollment Text for Mobile Payments

Then, when triggered by data submitted from the City, Pay Connexion will alert the payer via text message that a payment is due and provide the payer with the option to make a payment using the account that was designated at the time of mobile enrollment. If confirmed by the appropriate text response, the payer will receive a Payment Confirmation text as well as a Payment Confirmation email.

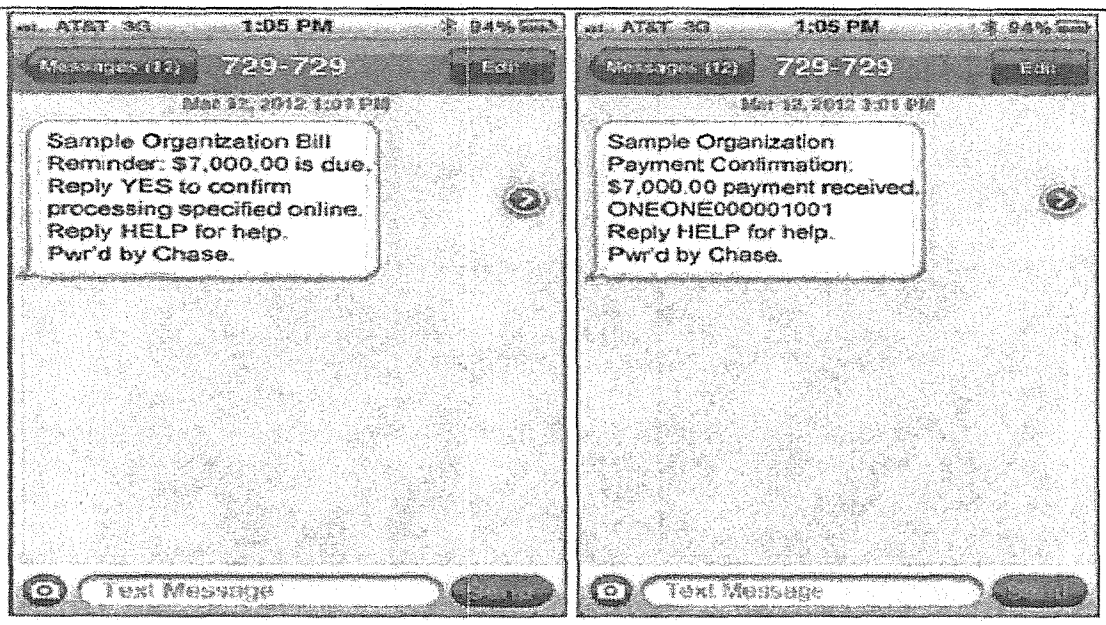


Figure 6. Sample Payment Confirmation Text for Mobile Payments

Additionally, as long as the mobile device utilizes a supported web browser (Microsoft Internet Explorer version 6.0, 7.0, 8.0 or Firefox 3.0, 3.5 or Google Chrome 3.0 or Safari 4 or 5) and/or DTMF telephone the Pay Connexion web and/or IVR channels (respectively) may be utilized.

F379	**Payment Type (Cash, Check and Money Order):** The system should accept the receipt of cash, check, money order, and wire transfer.	Describe how the system supports the receipt of cash, checks, money orders and wire transfers. If the system does not support these payment types then provide a detailed description of how the system integrates with other vendor systems that do provide this capability.	Expected

J.P. Morgan's Pay Connexion is a secure, multi-lingual, highly-available, fully-bank-hosted, PCI-DSS compliant multi-channel e-payment platform that supports credit and debit card, as well as ACH/e-check payment methods. It is a system designed to facilitate electronic web based payments and as your depository bank, J.P. Morgan has solutions to facilitate the acceptance of in person transactions of cash, checks, money orders and wire transfers. J.P. Morgan would like to consult with the City of the best practice use of services focusing on paper processing, which may include Lockbox, remote check capture, and branch or vault services for currency deposits.

Alternatively, the City may develop its own mobile applications as needed which will collect payment account information and transmit it to Pay Connexion's via Web Services API methods for processing. This model provides the City with tremendous flexibility with respect to application development. Please note though that because in this model the City collects payment account information from the payer and transmits it to Pay Connexion, the City would bear more of a PCI-DSS compliance burden than in the model in which the payer enters payment account information directly into Pay Connexion.

F393	**Payment Channel (Third Party Vendors):** The system may support online credit card payments through Google Checkout and	Describe what third party vendors the system supports to process online credit card transactions.	Desired

	Amazon Accounts.
Pay Connexion only uses our "in-house" merchant processor, Chase Paymentech to process and settle merchant transactions for card payments J.P. Morgan controls the entire lifecycle of an electronic payment – from the front end gathering of payment instructions from the payer via our Pay Connexion platform to settlement through our merchant processing company, Chase Paymentech. Maintaining the collection of information and subsequent settlement of payments under a single umbrella allows J.P. Morgan to avoid the use of third-party operators and boost efficiency. Pay Connexion does not utilize third parties for processing, and neither supports Google Checkout nor Amazon Accounts.	

F530	**Real Time Transaction Error Feedback:** The system may provide immediate online notification to the user of erroneous transactions.	Describe how the system communicates the reason for the error to the users and how the error can be corrected.	Desired
Pay Connexion provides payers with real time error feedback in such a manner that does not undermine security. For example, if data entered either is invalid (e.g., Payment Amount includes alpha characters or does not conform with configured business rules as defined by the City (e.g., is not between the City's defined minimum and maximum payment amounts, or Scheduled Payment Date is after the Payment Due Date) then the payer is presented with a message in real time advising of the specific error. In the event that a card transaction is declined, (e.g., the card was reported to the issuer as lost/stolen, the expiration date has past, Address Verification Service or Card Verification Data checks resulted in response codes that are not accepted per the City's rules, etc.) then a message is presented to the payer in real time indicating that the transaction cannot be processed. The message is intentionally vague so as to not help an individual attempting to commit fraud refine his/her efforts.			

Reconciliation Requirements

Req#	Requirement Description	Required Response	Rating
F404	**Scope of Reconciliation:** The system must reconcile online transactions between the bank and the general ledger.	Provide a detailed explanation of how the system supports reconciliation initiated by the online payment transaction through the bank to the general ledger.	Expected
The City has the following options to receive remittance data: 1. Standard Daily Remittance File – Standard Pay Connexion-formatted remittance files are available to authorized administrative users for download through the administrative site for two weeks (14 days) after the file is posted. The standard remittance file is also available via file transfer protocol (FTP) if defined during implementation. Batch Remittance File is the primary method for Pay Connexion to communicate payment activity back to our customer's systems. The remittance file contains all of the processed transactions for the previous business day as well as ACH Returns, and is the data of record to be used for transaction reconciliation. The remittance file is also rich with data which can be used for research, analysis and customer support purposes. The remittance file can be generated daily (excluding weekends, excluding Saturdays, or seven days per week) excluding US Federal Reserve holidays. The remittance file has a standard file layout, which can include City-defined data parameters, and can be sent as a CSV or XML file. The remittance file is generated at the biller-level in the Pay Connexion logical hierarchy and contains transactions via all supported payment channels and payment methods for the application, as well as ACH returns. Remittance Files include the data needed for reconciliation since they reflect the transactions in the			

ACH and card batches that closed since the prior remittance file.

2. Real Time Payment Confirmation (RTPC) – Our fully hosted Pay Connexion application can process and send payments to the City in real time through the optional Real-Time Payment Confirmation (RTPC) interface. The RTPC feature allows the City, to receive real-time payment information each time a payment is initiated, edited, canceled, or refunded. This allows the City to update its systems in real-time and better facilitates making time-sensitive decisions. These messages are sent over the Internet via HTTPS Post, and are sent every day, including weekends and holidays, immediately upon completion of a payment action.

3. Manual Posting is available and is another means by which you can post payment activity to your systems. Authorized personnel can generate reports and/or download a remittance file (in a standard format) from the Pay Connexion administrative site.

Authorized City personnel can access the administrative application, which is a robust customer service and payment reporting tool. All pages within the administrative application are compliant with section 508 of the Americans with Disabilities Act. The site is accessed through a secure URL. Each session is secured using Secure Sockets Layer (SSL) with 128-bit encryption technology.

Security measures are paramount and required to validate access to the reporting site. City "security officers" dictate access to the administrative site by defining administrative site functions to City-defined role(s). The City then assigns individuals to each role. Individuals are also given secure user names and passwords to access the administrative application. Therefore, when an individual logs-in to the administrative site, they only see the functions necessary for them to perform their job.

Through Pay Connexion, the City will be provided with an online payment reporting tool to access your Daily Transaction Reports. Reporting capabilities are available through your administrative application, which allows you to view standard reports that include payment detail, payment summary, and credit card batch reports. Each report has different selection criteria that can be used to narrow the data of a selected report. The reports can be downloaded from the administrative application into Excel.

A daily remittance data file will be made available for download via the administrative site or through secure FTP. This remittance file is the primary means to deliver remittance detail to the City. This standard format includes return data as well, and provides a daily means (Monday through Friday, excluding Federal Holidays) to reconcile funds settlement. The file is available in Extensible Markup Language (XML) and ASCII comma-delimited variable length formats.

Authorized City administrators access the Pay Connexion administrative site from a standard web browser. The administrative site provides authorized City personnel with the ability to make payments, execute refunds (refund rules differ by payment method), generate a wide range of reports on demand, and perform other administrative functions.

Single Payments Section
- View Pending Payments
- View Payment History
- View Payment Details
- Make User Payment
- Refund Payment
- Cancel Pending Payment
- Edit Pending Payment
- Reactivate Payer for ACH Payments

Recurring Payments Section
- Make User Recurring Payment
- View Recurring Payments
- View Recurring Payment Details
- Edit Recurring Payment
- Stop Recurring Payment

Registered Payers Section
- Reset Registered Payer Password
- View Payer Profile
- Edit Payer Profile

Payment Accounts Section
- View Payment Account
- Delete Payment Account
- Enable Invalid Account

Customer Service Section
-Initiate Call (all customer service functions accessed through Initiate Call)

Administrative Reports Section
- Payment Detail Reports
- Payment Summary Reports
- Download Remittance File
- Download CSR Payment Reports
- Card Batch Reports
- Recurring Payment Reports
- Admin User Access Report
- Fraud Detection Report

Pay Connexion reports provide very flexible filtering capabilities by allowing your users to select parameters for downloading data. For example, reports can be run with specific date ranges, dollar ranges, product types (as applicable), payment types (card, ACH, etc.,) and payment channels (web, IVR, admin). By combining these various parameters, the City has the ability to narrowly define the specific data your wish to download. Reports can also be sorted by each of the columns displayed in the report results. The reports are either produced in batch or real time, and can be viewed online, printed, and downloaded (*.csv) to the desktop of the administrative user. The following types of reports are available through the administrative site:

- Payment Detail Report
- Product Detail report
- Payment Summary Report
- Recurring Payment Report
- Product Recurring Payment Report
- Card Batch Report
- Fraud Detection Report
- Administrative User Access Report
- Download Remittance File

Please see *Attachment 2* for sample Pay Connexion reports.

F405	**Exception Reporting:** The system must send notifications of exceptions to appropriate staff when a transaction does not reconcile.	Describe how the system reports on exceptions and how these notifications are routed and to whom (including back to departments). What is the lag time between event and notification?	Expected

Please see our response to *Req #381* regarding Chargebacks.

Payment detail and summary reports may be generated to view additional exceptions such as Returns, Refunds and Declines. Declines occur in real time with the payment attempt. Refunds occur on demand as executed by

the City's authorized personnel. The timing of ACH returns will depend on the City's configuration selections with respect to whether returns should be resubmitted, and if so how many times, whether resubmissions should be delayed and if so by how many days.

J.P. Morgan adheres to the following Severity Level-based approach to unscheduled Pay Connexion System Outage/service interruptions notification. The City is able to designate which individuals are to receive notifications. The City will be given a written notification of breach of a service level.

Table 3 - Incident Severity Level Definitions

Severity Level Definition	Initial Contact w/ Clients / Internal Functional Teams
Primary Definition: ▪ Severity 1 (Emergency) Degeneration in or complete failure of, the system or any single channel (Web, Admin) to receive and process payments. ▪ Restricted to true, system-wide emergencies. A complete failure has occurred in either a system or critical process.	15 min to Client contacts and/or Internal Functional Team Designate (TBD); hourly updates until resolved
Primary Definition: ▪ Severity 2 (High) Degeneration in, or complete failure of, business-critical secondary functionality (RTPC, all file processing, password reset, download a Remittance File, or the ability to initiate a call) for a single Biller or group of Billers ▪ Used when the problem is severely affecting a group of users. A major portion of a system or process is not functional, but can be bypassed, or it is a functional failure with no workaround.	15 min to Client contacts and/or Internal Functional Team designate (TBD); hourly updates until resolved
Primary Definition: ▪ Severity 3 (Medium) Degeneration in product functionality of non-critical tertiary functionality (confirmation emails, standard reporting, etc) for a single Biller or a group of Billers ▪ This is the most common severity level. A system or process is mostly functional but not performing as expected. An error can be ignored, or a workaround can be used.	Monthly issues log
Primary Definition: ▪ Severity 4 (Low) System or critical process is functional, but a problem exists related to ease of use (slow app response time or screen flows), interface or Standard Report content, or a problem exists for a single payer or group of Payers (can't reset passwords, can't log in). ▪ A single Payer is impacted. A system or process is currently fully functional but a problem exists, or the problem relates to information, process change(s), minor enhancement(s), or request(s) for future functionality.	Monthly issues log

F226	**Standard and Policy Enforcement:** The system should provide standards and processes to determine how transactions are recorded and reconciled.	Describe the standards and processes that the system supports to enforce how transactions are recorded and reconciled.	Expected

Regardless of the payment method used, if a payment transaction is authorized, a confirmation page is presented to the payer. This is the case for single payments, whether immediate or future-dated ("warehoused"), when non-payment initiation actions are executed (e.g., a payment is edited or refunded), and when instances of recurring payments occur. Recurring payment authorizations/instructions result in a unique recurring payment reference number. The confirmation page may be printed for a hard-copy receipt. The payer also has the option

of providing an email address (unless required by the City). If provided, the payer may have the payment confirmation sent via email. A unique Pay Connexion confirmation number is assigned to every payment made and provided to the customer upon payment submission. With a confirmation number, a payer will be able to view the payment initiation date, the date a payment was processed, the account number from which the payment was made, the payment amount, and the payment confirmation number. Once a payment is submitted, the customer can immediately "recheck" the status of their payment. The payment can be viewed on the payment site immediately following the payment.			
F401	**Three-way Matching:** The system should provide three-way matching capability between department system, credit card processor and bank deposits.	Describe how the system performs three-way matching.	Expected
Please see our responses to *Req #F377 and #F404.* Each day's remittance file is generated after the card and ACH batch close times and contains the transactions recorded in those batches, which are the transactions confirmed since the prior batches closed. Remittance files also contain ACH returns. Depending on the City's configuration requirements, Chargebacks may also be contained in the remittance file. Unless the City departs from recommended batch close time options, deposits representing the ACH and card batches are expected to reconcile with the respective subtotals for ACH and card payments in the day's remittance file. Additionally remittance file data is used for posting payment transactions to the City Department's back-end systems / general ledger. Thus deposits may ne expected to reconcile to the processed batches for card (processed through Chase Paymentech) and ACH (processed by J.P. Morgan) and to the City Department's back-end systems / general ledger.			
F253	**Transactional Cross-referencing:** The system should perform transactional cross-referencing where a user can perform a query to locate the details of associated transactions in the processing "chain" of transactions.	Describe the system capabilities to locate specific events within the entire transaction cycle.	Expected
Pay Connexion reports provide very flexible filtering capabilities by allowing your users to select parameters for downloading data. For example, reports can be run with specific date ranges, dollar ranges, product types (as applicable), payment types (card, ACH, etc.,) and payment channels (web, IVR, admin). By combining these various parameters, the City has the ability to narrowly define the specific data your wish to download. Reports can also be sorted by each of the columns displayed in the report results. Pay Connexion supports unique transaction identifiers that may be used to cross reference across the processing chain of transactions. ACH Trace Numbers and card Authorization Numbers are recorded and associated with each ACH and card payment (respectively) in the Detail Record of the remittance file, which also contains the Pay Connexion-generated unique transaction confirmation number for each payment transaction. These numbers may be used to cross-reference when researching the processing details of a payment with either J.P. Morgan ACH or Chase Paymentech. Further, if required in researching a transaction, logs may be requested from the Operations Practice Management team detailing data that was transmitted between City, Pay Connexion J.P. Morgan ACH and Chase Paymentech.			
F102	**Transaction Mapping Notation**: The system should allow internal or external user to add notes to a transaction (i.e. special	Describe how information is stored in the system, the length of note fields or text boxes, including any editing capabilities.	Expected

	instructions, rationale for mapping two disparate transactions together for reconciliation and insertion into general ledger)		

If Req #F102 refers to post-payment annotation, then please see our response to *Req #404*.

Pay Connexion remittance files are not editable in Pay Connexion itself, which preserves their integrity of these file for audit purposes. Therefore, Pay Connexion does not provide the ability for a payer or administrative user to modify a payment after it has been made. Typically, clients either develop interfaces as needed to import data from the remittance files into their back-end systems or post and reconcile payment manually from the remittance file. It is expected that post-payment transaction annotation can occur either in a City-developed interface or where the City downloads the remittance file as a *.csv file and annotates it as needed outside of Pay Connexion (e.g., in MS Excel).

If Req #F102 refers to annotation required during the payment process, then Pay Connexion can support collected parameter fields in which the payer may enter brief notes while making a payment. Please note that collected parameters may be defined during the Configuration Requirements Definition phase of implementation under the "product" level of the Pay Connexion logical hierarchy. Also note that using collected parameters for this purpose during IVR payments may be impractical due to the constraints of a telephone keypad for data entry.

F529	**Error/Suspense File:** The system should control the correction and/or reprocessing of all erroneous transactions by using of error/suspense files. Erroneous transactions to be maintained until corrected and posted.	Describe how suspense file transactions are processed and what controls are in place to ensure an accurate posting process.	Expected

Please see our response to *Req #404*.

Pay Connexion remittance files are not editable in Pay Connexion itself, which preserves their integrity of these file for audit purposes. Pay Connexion does not provide an error/ suspense file. Typically, clients either develop interfaces as needed to import data from the remittance files into their back-end systems or post and reconcile payments manually from the remittance file. It is expected the City will utilize a City-developed interface or download the remittance file as a *.csv file and post/reconcile as needed outside of Pay Connexion (e.g., in MS Excel).

F402	**Subsidiary Transactions:** The system may provide detailed subsidiary transactions that are compared with the general ledger. A report is then created showing this, resulting in the creation of reports of accounts that are out of balance.	Describe the report writer within the system and the ability to export data to other formats. (Specify data file types) What frequencies can be defined by the user? (e.g. daily, weekly and monthly)	Desired

Please see our response to *Req #F404*.

F454	**GL String Exception Reporting:** The system may provide exception reporting for general ledger strings coming from department systems that do not match the GL structure.	Describe how the system handles exception reporting for GL strings that do not match between the department system and the GL.	Desired

Please see our response to *Req #404*.

Pay Connexion remittance files are produced in a standard Pay Connexion format. Typically, clients either

develop interfaces as needed to import data from the remittance files into their back-end systems or post and reconcile payments manually from the remittance file. It is expected the City will utilize a City-developed interface or download the remittance file as a *.csv file and post/reconcile as needed outside of Pay Connexion (e.g., in MS Excel).			
F455	**GL to Department Reconciliation:** The system may enable automatic reconciliation between the GL and individual department systems. (e.g., automated revenue validation process).	Describe the process the system uses to automatically reconcile the GL with individual department systems.	Desired
Please see our response to *Req #404*. Pay Connexion remittance files are produced in a standard Pay Connexion format. Typically, clients either develop interfaces as needed to import data from the remittance files into their back-end systems or post and reconcile payments manually from the remittance file. It is expected the City will utilize a City-developed interface or download the remittance file as a *.csv file and post/reconcile as needed outside of Pay Connexion (e.g., in MS Excel). Pay Connexion remittance files are generated at the "Biller" level in the Pay Connexion logical hierarchy, which in client environments similar to the City of Austin's (as outlined in this RFP) typically aligns to a Department.			

Auditing Requirements

Req#	Requirement Description	Required Response	Rating
F134	**Audit Log Query:** The system must enable query of the audit log in real time.	Describe how the system enables the audit log to be searched (ex. By access type, date/time stamp range, department, user ID, or terminal ID, type of transaction)	Expected
Please see our response to *Req #F404*. Pay Connexion captures transaction details in real time as payments are confirmed (or declined). The audit trail for each transaction includes the payment channel, payment method, payment confirmation date/time, payment status and more. This information is available for authorized administrative users who may either search for payment details, payor details (for registered payers) or generate payment detail reports all in real time and/or research information in the batch remittance file, card batch reports (detail/summary) or use other reports or files as applicable for the configuration. Pay Connexion's reporting section of the administrative application provides billers with the ability to create various detail and summary level payment reports. Administrative users must be granted permission to access each type of report. Payment reports can be generated for pending and processed payments and can be filtered by various fields, including payment method, payment type, product, and payment status. Reports can also be sorted by each of the columns displayed in the report results. The reports are either produced in batch or real time, and can be sorted, viewed online, printed, and downloaded to the administrative users desktop. During the Configuration Requirements Definition phase of implementation the City will be able to define Administrative Organizations as needed. Admin Orgs align to a Biller or set of Billers within the Pay Connexion logical hierarchy. Thus, for example if each City Department has its own "Biller", there could be a corresponding Department-specific Admin Org, as well as an overarching multi-Department Admin Org for admin users that require admin access across Departments. City designated "Security Officers" will define administrative roles that map to City job functions and will manage individual admin users who serve in those jobs. With this structure, the City is able to define and manage administrative access on a department/domain based basis, role-based basis			

and individual-based basis.

Authorized City administrators access the Pay Connexion administrative site from a standard web browser. The administrative site provides authorized City personnel with the ability to make payments, execute refunds (refund rules differ by payment method), generate a wide range of reports on demand, and perform other administrative functions.

Authorized personnel access the administrative site through a secure URL. Each session is secured using Secure Sockets Layer (SSL) with 128-bit encryption technology. Authentication is required for customer service representatives and administrators to access to the administrative site. All data is stored securely. This easy yet secure access to transaction and other information is ideal for efficient customer support and issue resolution. In addition, an online context sensitive 'Help' utility is available to administrative users.

Transaction history is saved for 24 months (2 years) online, and an additional 5 years offline. By law, we are required to save this information for 7 years.

F178	**Transaction Tracing:** The system must provide audit trails to trace transactions from their initial source through all stages of system processing.	Describe how the system traces transactions from start to finish and specify the fields it can trace.	Expected

Please see our responses to *Req #F134, #F253 and #F404.*

Remittance file detail record field names include the following. Please note that not all fields will apply to every configuration or transaction, and note that other files and reports are also available that augment the audit trail.

- Payment Reference Id
- Transaction Confirmation Id
- Payment Reference Id
- Biller Product Code
- Amount Due
- Payment Amount
- Convenience Fee
- Total Amount
- Biller Business Date
- Payment Effective Date
- Initiation Date
- Payment Type
- Card Type
- Payment Authorization
- Payment Status
- ACH Return Code
- Reason Description
- Return Date
- Chargeback Amount
- Chargeback Activity Date
- Access Method
- First Name
- Last Name
- Company Name
- Country Code
- Phone
- International Phone
- Street Address 1
- Street Address 2
- Street Address 3
- City
- State Code
- Province Name
- Zip Code 5
- Zip Code 4
- Postal Code
- Email
- Sales Tax Amount
- Customer Reference Number
- Parameter Name (1...N)
- Parameter Value (1...N)
- Statement Number

▪ User Id			
F177	**Audit Log:** The system should maintain an audit log that records all additions, modifications and deletions of data (including security permissions) made by individual users to specific field level data elements.	Describe how the system keeps track of additions, modifications and deletions of individual data elements by user.	Expected
Please see our response to *Req #F172*. Also note that administrative user activity in the administrative site is automatically logged for audit purposes.			

Reporting Requirements

Req#	Requirement Description	Required Response	Rating
F131	**Report Data:** The system should support direct real time access to current year and historical billing/sales data going back 36 months.	Describe how the system supports direct real time access to current and historical data.	Expected
Please see our response to *Req #404*. Transaction history is saved for 24 months (2 years) online, and an additional 5 years offline. By law, we are required to save this information for 7 years.			
F451	**Standard Reports:** The system should allow users to create standard transaction reports.	Describe the system reporting capabilities, including management information reporting, summary reporting, and detail level reporting. Provide sample reports. What are the standard delivery formats?	Expected
Please see our response to *Req #404*.			
F453	**Customized Reports:** The system should allow users to create customized transaction reports.	Describe options to create customized reporting. How often can reports be generated? Describe the process to build reports.	Expected
Please see our response to *Req #404*.			
F130	**Report Preview:** The system should provide the ability to preview a report, form, or other query result before printing.	Describe the report preview features that the system provides.	Expected
Please see our response to *Req #404*. When generating a report authorized admin users are given the option to view the report results online or download them. This enables the user to preview a report online before running a report against the same criteria and downloading report results.			
F126	**Report Library:** The system should allow users to create and save parameter-based query scripts and reports for storage in a	Describe how your system enables the creation, organization (ex. By user, group, report type) and maintenance of a central	Expected

	central library for future use.	repository of reports.	
Please see our responses to *Req #404 and Req #F134.* Reports may be downloaded, should a central repository of reports be required.			
F129	**Report Data Export:** The system should enable authorized users to download billing/sales data in a variety of common formats.	Describe the supported formats (e.g., ASCII, Excel, CSV formatted).	Expected
Please see our responses to *Req #404 and Req #F134.*			
F477	**Transaction Fee Reporting:** The system should provide the ability to report on fees.	Specify if this is a standard or custom report.	Expected
Pay Connexion does support as a standard option the ability to generate Payment Summary, Payment Detail and Product Detail Reports on payments, convenience fees or both.			
F127	**Automated Report Generation:** The system may allow users to run reports or queries either online or in batch mode and to stage output for later access by authorized users.	Describe the capabilities the system provides to run online or batch reports and stage the output for later access by authorized users.	Desired
Please see our response to *Req #404 and Req #F134.* Report results are retained for four days allowing authorized users to review them repeatedly within that time frame without having to re-generate the same report. Additionally, because reports may be downloaded, authorized personnel are able to archive report results as needed. Transaction history is saved for 24 months (2 years) online, and an additional 5 years offline. By law, we are required to save this information for 7 years.			
F128	**Report Formatting:** The system may provide graphical formatting capabilities.	Describe the report formatting capabilities of the system.	Desired
Please see our responses to *Req #404 and Req #F134.*			
F132	**Report Distribution:** The system may enable users to automatically distribute copies of reports and query results.	Describe how the system can distribute reports (email or portal based), multiple pre-defined individuals or groups.	Desired
Reports are not distributed from Pay Connexion by email, however, once downloaded by an authorized admin user, reports may be distributed internally as needed by the City.			
F133	**Report Functions:** The system may provide an active data dictionary to provide users with object definitions, and online help.	Describe additional reporting functions that your system provides including an active directory and online help.	Desired
Pay Connexion provides a robust context-sensitive online help facility that is available 24/7, 365 days for payers and administrators with step-by-step instruction for using the application.			

TOC

- Welcome
- Using Application
- Make Payment
  - Make a Payment
  - Pay Without Registering
  - ATM Card Account Information
  - Payment Type and Method Selection
  - Payment Verification
  - Payment Confirmation
- Enroll with Mobile Text
- Payment History
- Pending Payments
- Manage Accounts
- Recurring Payments

TOC

Favorites

You are here: Make Payment > Make a Payment

MAKE A PAYMENT

Topic:

The Payment process can vary, therefore you may or may not see all of the features covered in this section.

Explanation:

STEP 1: Enter **Payment Information**

- This section will display if there is additional information to be displayed or requested for your payment.
- Complete the requested information, required fields will display in bold type. There can be multiple fields and they can consist of data entry, drop-down list, radio buttons, or a combination.
- If available, Statement Information will be displayed in this section.
  - If an Image is available for the statement, you can click the statement number link to see more details.
  - If used, the "Filter by" menu will show only the statements with a status you pick from the Filter drop down menu.
  - Click the page numbers to see more statement rows.
  - If you click an underlined column header, the rows will sort ascending using that column. If you click the same column header again, the rows will sort descending.
- A link to download Acrobat Reader is also available on this screen.

TOC

- Welcome
- Reports
- Make Payment
- View Mobile Text Enrollments
- Admin Access
- Payment Information
- Account Information
- General Information
  - View Job Role
  - View Job Role - All Roles
  - Login
  - Logout - Confirmation
  - Logout - Exit
  - Browser Requirements
  - Main Menu
- Subscription Info
- Page Definition

TOC

Search

Favorites

You are here: General Information > Main Menu

Main Menu

Topic:

The **Main Menu** lists the tasks you are authorized to perform. You may see one to many of the following options. Select the link for the task you would like to perform.

Explanation:

MANAGE ADMINISTRATIVE USERS

This section allows you to add, edit, and delete administrative users and reset admin users' passwords. An **Administrative User** is any individual in your organization that requires access to the system. **Please Note** that administrative roles must be defined before you create your administrative users.

- Create Admin User allows you to add a new admin user to the system.
- Edit Admin User Profile allows you to modify the profile information, including email address, phone number, and title for an existing admin user.
- Disable Admin User allows you to remove an admin user from the system if they no longer require access to the system. Please Note that once an admin user is disabled, their account can't be re-enabled and the username can't be re-used.
- Reset Admin User Password allows you to reset an admin user's password if they have forgot their password or locked their account.
- Manage Admin Hierarchy allows you to assign administrative users to a hierarchical structure for reporting and tracking purposes.

MANAGE ADMINISTRATIVE ROLES

This section allows you to add, edit, or delete Roles. A **Role** defines the permissions that an admin user can perform and may contain one to many permissions for the admin user(s) that will be assigned to the Role.

- Create Admin Role allows you to add a new role to the system.
- Delete Admin Role allows you to remove a Role that is no longer necessary.
- Edit Admin Role allows you to modify an existing role to add or remove permissions.

CUSTOMER SERVICE

This section allows you to manage payors and payments. Select **Initiate Call** to

A 24/7, 365 day live support option for payers is available at additional cost. We recommend the City provide a support phone number and hours of operation within the Pay Connexion line help menu.

Interface Requirements

Req#	Requirement Description	Required Response	Rating
F104	**Transaction Metadata:** The system must track specific details for each payment transaction.	Describe the core metadata your system can capture, track and maintain at the individual transaction level. Explain how configurable this capability is. Provide samples of key data that is typically captured by some of your existing clients.	Expected

Pay Connexion makes a suite of standard product interfaces available to clients. These use IT-industry standards (e.g., Web Services (SOAP) API, ASCII files, XML, HTTPS Post). Clients utilize these standard Pay Connexion product interfaces when integrating client systems with Pay Connexion. Which specific Pay Connexion product interfaces any client application utilizes, as well as how each is configured is determined during the Configuration Requirements Definition phase of implementation. The determination of which interfaces will be "in scope" and how each is used may be based on factors such as:

- Which specific Pay Connexion features each application requires (e.g., some applications require the Recurring Payments File, Real Time Payment Confirmation, Statement Image Archive File, etc. whereas others do not)
- How certain Pay Connexion features will be utilized (e.g., which records types in the Pre-Registration File and fields in a given record type are utilized is configuration driven)
- The City's technical preferences (e.g., whether the Remittance File is *.csv or XML)

The following represents the sort of data that Pay Connexion can capture, track and maintain at the individual transaction level in the remittance file, and representative data is provided for the payment of a parking citation by an unregistered payer.

Table 4 - Pay Connexion Data Samples

Data	Example
Transaction Confirmation ID	ABCDEF000001234
Payment Reference ID	
Product Code	Parking Citation
Amount Due	$100.00
Payment Amount	$100.00
Convenience Fee	$1.00
Total Amount	$101.00
City's Business Date	5/29/12
Payment Effective Date	5/30/12
Payment Initiation Date and Time	5/29/12 1:27:00 PM
Payment Method	ACH

Card Type	
Payment Authorization	12341234
Payment Status	SENT
ACH Return Code	
ACH Return Reason Description	
Ach Return Date	
Chargeback Amount	
Chargeback Activity Date	
Payment Channel	WEB
User ID	
First Name	John
Last Name	Doe
Company Name	
Country Code	USA
Phone	(555) 555-5555
International Phone	
Street Address 1	100 Main St.
Street Address 2	#101
Street Address 3	
City	Austin
State	TX
Province	
Zip Code 5	55555
Zip Code 4	
Postal Code	
Email	john.doe@noemail.com
Sales Tax Amount	
Customer Reference Number	
Parameter Name (1...N)	Citation Number
Parameter Value (1...N)	ABC-12345
Statement Number (1...N)	
Statement Payment Amount (1...N)	

F120	**Administrative Table:** The system must provide an interface table for mapping individual transactions received from department systems to the merchant processor, bank and general ledger.	Describe how the system maps individual transactions to batches and general ledger entries.	Expected

Pay Connexion remittance files are generated on a daily batch basis at the Biller-level in the Pay Connexion logical hierarchy and have unique identifiers representing the corresponding Biller Group and Biller. Thus, for example assuming each Department has a dedicated "Biller" then each Department will have its own Remittance

File. Remittance files contain detailed information about individual transactions (Please see our response to Req #F120 above) of the most recently closed ACH and Card payment batches. Detail for each transaction includes the Product Code identifier. The settlement DDA can be designated at the Product-level within each Biller (e.g., within a Parking Enforcement Department products might include Parking Citation, Towing Fee, Wheel Boot Release Fee, etc.) and may differ by Payment Method (e.g., card versus ACH) or may be aggregated at higher levels as needed. Deposits will be made by payment method and as defined (e.g., at the Product Level, Biller Level etc) and will support unique identifiers.

During the Configuration Requirements Definition phase of the implementation process, J.P. Morgan will work with the City to define the Billers, and products batch close times, as needed to achieve the appropriate data segregation/access.

F209	**Authorized Data Transmission:** The system must ensure that only complete and non-duplicated data is transmitted by an authorized sender to an authorized receiver.	Describe how the system accomplishes this process including how erroneous or flawed transactions are handled between the system, individual department systems and the General Ledger. Controls over each file should ensure (1) the number of transactions in the file matches control records; (2) the dollar total of transactions in the file matches control records.	Expected

Pay Connexion interfaces are designed and tested such that complete data is transmitted and duplicate data is not. System monitoring measures are in place. Should any erroneous or flawed transactions be detected, The Client Service / Operations Practice Management team will notify the City and coordinate root cause analysis and remediation as needed. Remittance Files contain counts of the number of transactions as well as the sum of the transaction amounts of payments and ACH returns that are detailed in the file, and optionally may include the same for convenience fees and chargebacks.

Pay Connexion includes logic to help prevent payers from making duplicate payments. The exact logic utilized varies with the application configuration, payer type (e.g., registered / unregistered), and payment type. If the payment being made currently seems to duplicate a recent payment, then the payer is advised and is given the opportunity to cancel or continue with the payment.

F121	**Transferring Files via Relevant APIs:** The system should broker inputs and outputs of transferable files to meet the relevant Application Program Interface (API) specified by departmental systems at the City.	Describe how the system brokers inputs and outputs via relevant APIs.	Expected

Pay Connexion interfaces include a variety of inbound and outbound file types, Web Services API methods and responses, and in and outbound HTTPS Posts. Each Pay Connexion application is configured during the Configuration Requirements Definition phase of implementation. During this phase, the specific interfaces that will be in-scope for the application, as well as the particular details of how those interfaces will be used, is determined. The application is built to utilize the in-scope interfaces. If use of out-of-scope interfaces are attempted, or the particulars of an in-scope interface are invalid and do not conform to the Configuration Requirements-driven Build, then Pay Connexion disallows the action that was attempted and returns an appropriate.

Pay Connexion offers the option for the City to host the payment channel through Pay Connexion's gateway. Pay Connexion's gateway allows the City to host payment channels and send payment data through Pay

Connexion's API/Web Services.

Pay Connexion's API is built on top of J.P. Morgan's payments infrastructure and provides the City with additional options when determining the appropriate way to integrate and share data between applications.

Pay Connexion's API maintains a set of components around the following:

- Making and managing payments
- Creating and managing payment accounts
- Creating and managing payer profiles

Every component contains a request message and response message. Therefore, a "real-time conversation" occurs between the City's system and Pay Connexion with the appropriate sharing of data.

Pay Connexion's API uses industry standards and best practices. These include:

- W3C – SOAP 1.2 - SOAP Lightweight protocol intended for exchanging structured information in a decentralized, distributed environment. This messaging framework uses XML technologies, an extensible messaging framework containing a message construct that can be exchanged over a variety of underlying protocols.
- WS-I Basic Profile 2.0 - This is a set of non-proprietary web services specifications, along with clarifications, refinements, interpretations, and amplifications of those specifications, which promote interoperability.

Every Biller that uses Pay Connexion's API will be required to follow the mutual authentication scheme. This involves the City installing a certificate on their server and J.P. Morgan installing a certificate on its Pay Connexion server. All messages will also be required to be sent over HTTPS. Therefore, you can be confident in the following:

- You, as the Biller, can be sure you're communicating with Pay Connexion
- Your communication with Pay Connexion is encrypted, so others can not intercept it
- You have verification that the message received relates to the message sent

Additional technical information is provided during Pay Connexion's implementation process.

F122	**Core Financial System Interface:** The system should interface with the core financial system to record transactions consistent with City posting rules utilizing existing XML standards.	Describe how the system can export transaction data to integrate with other systems.	Expected

Among the possible points of integration between our systems the City may potentially be sending payer information to us and we will be sending you remittance data about the transactions processed.

The City delivers to Pay Connexion payer profile and billing data, as well as images of bills, if required.

Pre-Registration File or some Web Services API methods are means for the City's systems to communicate payer profile (e.g., name, contact information, etc.) and billing data (e.g., ID number, amount due, etc.) to Pay Connexion. Use of pre-registration enables a variety of Pay Connexion features (e.g., electronic bill presentment, auto log-in, etc.). The pre-registration file and updates to it are sent in batch mode in a standard file layout and *.CSV format, which can accommodate the City's particular data elements or "parameters". The pre-registration file can be delivered to J.P. Morgan via secure FTP or a variety of other data transfer protocols.

Statement Image Archive File can be the means for the City's systems to communicate *.PDF images of bill statements themselves. We have the ability to present the bills on our system. These bill images correspond to the billing information provided in the Pre-Registration File. This file may be delivered as a .zip, .tar, and

.tar.gz file, and may be delivered by secure FTP or a variety of other data transfer protocols.

Payer information can also be sent to Pay Connexion through a Web Session Transfer (available for the Web channel only). Upon clicking the Pay Button(s), customers will be passed via a session transfer to our secure Pay Connexion e-Payment web site, on which they will be able to execute the e-Payment process. The session transfer can contain data elements unique to the payment type. For example, the City can send parameters or custom data (e.g., account number) in the session transfer. This data will be associated with each payment. This data is also included on the Remittance Batch File and real-time payment confirmation.

Pay Connexion transaction remittance data is delivered to the City's systems

Batch Remittance File is the most common method for Pay Connexion to communicate payment activity back to our customer's systems. The remittance file is generated daily Monday through Friday, six days per week (excluding Saturdays), or seven days per week, excluding Federal Reserve holidays. The remittance file has a standard file layout which can reflect the Biller's configuration, and can be sent as a CSV or XML file. This file can be delivered via secure FTP or a variety of other data transfer protocol, and is available for download by authorized personnel via the administrative site.

Real Time Payment Confirmation (RTPC) messages may be sent from Pay Connexion to the City's systems to communicate payment activity in applications that are too time-sensitive to be updated by a daily batch remittance file. RTPC allows your systems to receive real-time payment information each time a payment is initiated, edited, canceled, or refunded. As a result, the City will be able to make real-time system updates and time-sensitive decisions. RTPC messages are sent in a standard format that can reflect custom "parameters" real-time (including holidays and weekends) via the Internet, using http or https, and immediately upon completion of a payment action. RTPC messages are sent in a standard format that reflects your custom City-defined parameters/data.

The Remittance File and optional RTPC interfaces comprise the means by which transaction data may be communicated to the City's back-end systems.

F123	**Linking Merchant IDs to Batched Credit Card Transactions:** The system should identify the merchant ID for batched credit card transactions for which the deposit is being made.	Explain how the system identifies the merchant ID for batched credit card transactions for which the deposit is being made.	Expected

Please see our response to *Req #F120* above.

Merchant IDs (through which card payments are processed) as well as "Company IDs" (through which e-check payments are processed) may be defined at the "Product-level" in the Pay Connexion logical hierarchy. A Product Code identifier is associated with each transaction and correlates to a corresponding Merchant ID / Company ID. The settlement DDA that backs each Merchant ID / Company ID can be designated at the Product-level within each Biller (e.g., within a Parking Enforcement Department products might include Parking Citation, Towing Fee, Wheel Boot Release Fee, etc.) and may differ by Payment Method (e.g., card versus ACH). If the City prefers processing multiple "products" through common Merchant IDs / Company IDs, then Pay Connexion can support this aggregation at higher levels as needed. Deposits will be made by payment method and as defined (e.g., at the Product Level, Biller Level etc) and will support unique identifiers.

Security Requirements

Req#	Requirement Description	Required Response	Rating
F501	**Authorized System Access:** The system must limit system entry to authorized	Describe how system entry is limited to authorized individuals. Specify capabilities	Must Have

	individuals.	regarding user profiles and data security.	

Administrative organizations are groups of users that align to a set of Biller(s) in the Pay Connexion logical hierarchy. Administrative roles are established within each administrative organization. Roles are sets of administrative privileges that correspond to and enable the City to differentiate administrator access privileges hierarchically by job function. For example, if the City chooses, a Customer Service Representative (CSR) may only be enabled to view payments on behalf of a payer. A CSR Supervisor might have these privileges, and also be able to execute refunds. A CSR Manager might have the above abilities and be able to generate reports of transaction activity and CSR payment activity (for audit or productivity measurement purposes). An executive might have all of the above privileges and be able to download the remittance file. City designated Security Officer(s) will have the ability to manage the roles under each Admin Org. Thus, the City will be able to independently manage its administrative users' privileges both as job functions evolve and as staff turns over in these job functions. Access to the various administrative functions is granted only to users who are successfully authenticated. Passwords are assigned when a new administrative user is first granted a set of administrative privileges. Upon each administrative user's first successful log-in, the user is forced to establish a new password. Thus admin user access is managed on a secure, individual basis, role-based basis within designated domains as defined and managed by the City.

F503	**Limiting User Capability:** The system must limit the capability of users to: Selected functions Defined functional access rights Data access rights and Functional roles System administrators shall be able to add, delete, modify or change these user profiles at any time.	Describe how the system can limit access and functionality: Selected functions (i.e., create, read, update, and delete) Functional access rights (e.g., to modules, transactions and approval authorities) Data access rights (e.g., record, create, read, update and delete) Functional role (e.g., department admin) Describe the process the system administrator uses to add, delete, modify or change user profiles.	Must Have

Please see our response to *Req #F501* above.

City designated Security Officer(s) for e ach Admin Org will have the ability to manage the Admin Roles as needed. Thus, the City will be able to independently manage its administrative users' privileges both as job functions evolve and as staff turns over in these job functions. Access to the various administrative functions is granted only to users who are successfully authenticated.

F515	**Dual Administrative Rights**: The system must support dual administrative rights for assigning system user entitlements.	Describe how the system supports dual administration rights for assigning system user entitlements.	Expected

Please see our responses to *Req #F501 and #F503* above.

The City may designate one to many Security Officers for each Admin Org as needed. Security Officers have the superset of admin functions associated with the application(s) within the Admin Org, including the ability to manage Admin Roles and Admin Users. Because multiple Security Officers may be designated for each Admin Org, Pay Connexion supports dual admin rights for assigning system user entitlements.

F507	**Invalid Access Alerts:** The system must alert and record when invalid access is attempted or when user ID limit is exceeded.	Describe how the system alerts and records invalid access attempts.	Must Have

If the number of admin user authentication attempts under a specific admin User ID exceeds the allowable limit, then Pay Connexion advises the Admin User that his/her log-in credentials are locked. This activity is recorded and may be reported through the Admin User Access Report. At this point the Admin User must request a password reset. Password reset requests for most admin users are routed within a client's departmental team to the designated Security Officer(s) for the Admin Org. Security Officers request password resets through J.P. Morgan Client Service / Operations Practice Management team. In the password reset process, the admin user requesting the password reset, as well as the admin user (e.g., Security Officer) executing the password reset are both authenticated.

F508	**Alteration of Transaction Data:** The system must restrict the alteration of transaction data.	Describe how the system restricts the alteration of transaction data.	Must Have

Pay Connexion does not allow post-transaction modification of transaction related data.

F512	**Fraud Prevention:** The system must include measures for preventing fraudulent transactions.	Describe the protection and controls you offer to minimize fraudulent card use. How do you screen transaction activity for fraudulent patterns?	Must Have

Numerous components are incorporated throughout Pay Connexion to manage fraud risks. Most data is pre-populated and uneditable, account data is encrypted in storage and always masked when displayed, and Pay Connexion ensures appropriate authentication and authorization. J.P. Morgan and Federal ACH Directory databases are utilized to validate ACH Routing Transit Numbers in real-time. Daily Notices of Change are automatically incorporated when critical payment account data has changed, and payers can be automatically disabled from making eCheck payments after excessive returns. A daily Fraud Detection report identifies suspicious payer activity based on seven distinct criteria.

J.P. Morgan will implement leading practices and industry standard measures to prevent, limit, and detect fraudulent transactions. Among those that we will implement are:

- When possible and relevant, we perform format validations, such as maximum/minimum character lengths and character types, such as currency, alpha-numeric, all numeric, etc.
- Our system checks dates to ensure dates are valid and they are actual valid dates in the future
- Our system validates phone number to ensure they are numbers and include the appropriate length
- Our system validates e-mail addresses to ensure they are consistent format (e.g., X@Y.Z)
- Duplicate payment check (An error message informs the payer the payment now being made may be a duplicate of a recent payment.
- Mod-10 check performed on the card number
- Card number check to verify that it is a valid length for the card type
- Card number check to verify that it starts with correct digits for card type
- Verification that there are no spaces in the card number and all characters are numeric
- An expiration date check to confirm that the card has not expired
- For Signature debit cards and pinless debit cards a card number check against a Bank Identification Number (BIN file) is performed to make sure that it is a valid card

- Billing address zip code format check
- During the credit card authorization process, the following validation is performed and the payment is either authorized successfully or declined:
  - A payment amount check to make sure the payment does not exceed the available credit limit.
  - A stolen card check to confirm the card has not been reported stolen
  - A check to verify that the Issuer has not stopped all further payments on the card (placed by the card holder or the card issuer)
  - Address Verification Service (AVS)
  - Card Verification Data (CVD)
- Credit Card Authorization Attempt Limit (applies to the web only)

By utilizing our Pay Connexion platform, all credit and debit card transactions are protected by the industry leading security technology and procedures. J.P. Morgan's Pay Connexion solution is PCI-DSS compliant. We are continually making changes to our platform to conform to the ever-changing PCI-DSS standards. To review our certification, you can visit Visa®'s website at: www.visa.com/cisp. From that point, click on the "Service Providers" link and then the "List of CISP-Compliant Service Providers" link in the gray box to download the file that shows "Pay Connexion" as compliant. Please note that the card brands do not compile the report. A certified third party audit firm (in our case, Jefferson Wells) compiles the report. The card brands then approve or reject the report.

F511	**Fraud Prevention:** The system should protect the City from fraudulent charges incurred from stolen, fraudulent card activity or multiple attempts to hack the system by entering repeated fraudulent transactions.	Describe what happens if fraudulent charges are incurred before a card is reported missing. This is especially important if your solution includes a merchant processor.	Expected

Among the criteria that lead to the authorization of a card transaction is that the card has not been reported to the issuer as being stolen. Once a card has been reported lost/stolen, issuer will decline subsequent requests for authorization. In the event that a transaction is authorized after a card has been lost/stolen but before it has been reported to the issuer as being lost/stolen, a transaction may be processed. Please note that the payer will be able to contest such a fraudulent transaction(s) by initiating a Chargeback with the issuer.

The Chase Paymentech Chargeback Department will work with the Biller to evaluate every disputed charge. If Chase Paymentech is unable to remedy the chargeback, we send it to you with all supporting documentation. You may then research the transaction for a possible remedy. Included in each chargeback package is a merchant recourse form, which outlines the nature of the chargeback and the information required to reverse it. Chase Paymentech's chargeback support will ensure that this impact is minimized.

Additionally, refunds may be executed by the Biller's authorized personnel via the Pay Connexion administrative site. Depending on the City's requirements, authorized administrative users can recall transactions, and execute full and/or partial refunds with/without refund of the convenience fee.

Chargeback retrievals are a request for information from the issuing bank. They are typically initiated upon a cardholder's request. If the cardholder does not recognize a charge on their billing statement, they may contact their bank and request further information. This is done as a Chargeback Retrieval Request. Chase Paymentech receives retrieval requests electronically as part of their daily incoming chargeback files. They are matched against the Order History Database and a facsimile draft is produced which is either mailed or imaged to the initiating issuing bank.

Chargeback retrieval requests are also delivered to the merchant in order to obtain the required proof of the transaction. The printed proof of the transaction is then attached to the document and forwarded to the Issuer. According to Visa and MasterCard Operating Regulations, an acquirer (i.e., Chase Paymentech) has 30 calendar

days from the date received to fulfill a chargeback retrieval request (also referred to as a "request for copy"). Merchants are given until day 16 of the 30-day lifecycle to fulfill ticket retrieval requests. If a request is unfulfilled as of Day 14, Chase Paymentech will send a second request via fax, provided that the merchant is set up for fax delivery of their retrieval request notifications.

Generally, if a retrieval request is not fulfilled (i.e., copy of receipt is not presented), the retrieval becomes a chargeback. Facsimile and scanned images are acceptable means of producing the requested drafts.

Chase Paymentech ensures that operating procedures for exception processing, including retrievals and chargebacks, minimize Biller impact while addressing cardholder issues. Chase Paymentech's processing rules are written to generate a retrieval or chargeback response without Biller involvement if the required information is accessible by Chase Paymentech.

F513	**Fraud Prevention**: The system should provide configurable transaction limits for payment transactions.	Describe the controls that are available with your system to enforce per transaction or monthly transactional thresholds.	Expected

Pay Connexion supports configurable payment maximum and minimum payment amounts for each Product in the Pay Connexion logical hierarchy. The specific maximum and minimum payment amounts will be determined on a product-basis during the Configuration Requirements Definition phase of implementation.

F518	**User Identification Verification:** The system should provide a means of verifying the identity of users.	Explain how the system verifies the identity of users. Describe how configurable the capability is, how information gathered is kept secure and how the integrity of verified users is maintained over time.	Expected

There are three registration options from which to choose. First, the City may **pre-register** all of the end users through a Pre-Registration file and/or Web Services API method. In this case, the City would send user data in a daily or on-demand standard Pay Connexion formatted Pre-Registration file and/or Web Services API method. Updates to this file may be sent to J.P. Morgan via "delta" files. A Pre-Registration file reduces the number of users that will have to self-register upon entering the web site for the first time.

The use of pre-registration enables use of some of Pay Connexion's more sophisticated, albeit more complex, features, such as:

- Electronic Bill Presentment feature set
- Variable Recurring Payments
- IVR payment channel - Due to the limitations of a telephone keypad for data entry, pre-registration is required.
- The "Auto Log-in" feature can be used to further enhance the seamlessness of the user experience for payers that may have logged-in on the City's web site while maintaining security.

In applications that utilize pre-registration the City may choose to manage the payer's User ID and Password, or may provide an initial password and allow or force the payer to revise the password upon initial log-in.

Pre-Registration is frequently used in applications in which the payers' profile data is managed within the biller's systems (e.g., utility account holder).

In many applications, Pay Connexion customers do not have:

- The need for these features, or
- Sufficient information about payers or the technical ability to use pre-registration.

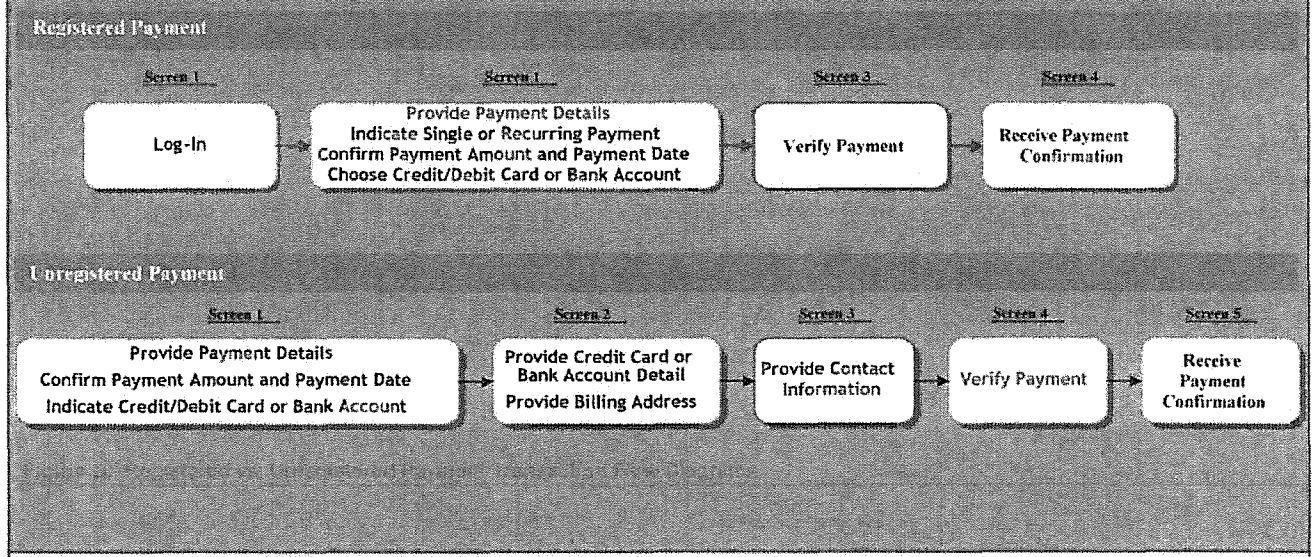
The second registration option is **self-registration**, whereby the end payer will be prompted to supply required information (e.g., name, e-mail address, account information) and to create a user name and password for verification purposes. Each time this end user makes a subsequent visit, the payment system recognizes them by their user name and password.

Additionally, registration allows the end payer to schedule recurring payments (configurable option necessitated by organizational needs) by indicating the payment amount, the accounts from which payments are to be drawn made, the frequency on which payments will be made, when payments will be initiated, and when the recurring payments will conclude.

With self registration, the payer manages his/her own profile, including the self-defined user ID and password.

A shared secret value is utilized for additional authentication purposes of both pre-registered and self-registered payers and may be used in scenarios such as when a password reset is required or customer service call is initiated.

The final registration option allows for an **unregistered** user to simply make a one-time e-Payment. Users will be required to enter standard transaction data each and every time they wish to make a payment. The standard profile data is not stored within the application and will not recognize the user upon future entries to the payment site. One-time payments are initiated by entering agreed upon identification information and their payment information (e.g., credit card information, or routing transit and bank account numbers). Unregistered users can access the completed one-time payment data with the confirmation number provided upon successful payment submission.



F502	**Configurable Access Windows:** The system may control access via configurable time windows.	Describe how the system supports configurable access time windows.	Desired

Pay Connexion's Web channel is accessed when a payer clicks on a Pay Button on the City's web site. If the City seeks to restrict payer access to the pay button to City-defined time windows (e.g., 9:00 am -5:00 pm Monday – Friday, June 1 – July 31, etc.) then the City must control the time windows during which the Pay Button is presented to payers. When the City does not present the pay button to payers, payers cannot access Pay Connexion.

During the Configuration Requirements Definition phase of implementation, the City will select the means by which payers will access Pay Connexion's IVR channel (if applicable). The available options include access via a transfer from an existing City IVR or PBX/switch or by dialing directly into a Toll Free Number. If access is limited to the transfer methods, then the City will be able to restrict the time windows during which Pay Connexion may

be accessible to payers.

Merchant Processor Requirements

Please note that these requirements only apply to vendors that are submitting their own merchant processor in their response. The City currently has a contract with Chase Paymentech.

Req#	Requirement Description	Required Response	Rating
F201	**Regularly Scheduled Transaction Files:** The merchant processor must make regularly scheduled credit card transaction files available to the City.	Describe what regularly scheduled transaction files are or can be sent to the City from the merchant processor and describe frequency options.	Must Have
Please see our response to *Req #F404*. Remittance file timing options will be discussed in detail with the City during the Configuration Requirements Definition phase of Implementation. The optimal timing will be determined in consideration of other related requirements such as which processing platform will be utilized, card and ACH batch cutoff times and other factors.			
F203	**Unique Transaction ID:** The merchant processor must assign a unique ID to each transaction.	Describe how the merchant processor assigns a unique ID to each transaction.	Must Have
Pay Connexion assigns a unique payment confirmation number to each transaction. Additionally, Chase Paymentech assigns a unique Authorization Number to each transaction. Both values are presented in the payment detail record for each transaction represented in the Pay Connexion remittance file.			
F533	**Credit Card Validation:** The merchant processor must determine that the account number is valid, the credit card has not expired, and there is sufficient credit available to cover the charge. Any credit card transaction that does not meet these criteria will be declined.	Describe the process the merchant processor uses to determine the validity of a transaction. Describe expected response times.	Must Have
Please see our response to *Req #F512* above. From the Pay Connexion payer perspective the authorization/decline response time does not exceed three seconds.			
F210	**Settlement of Valid Transactions:** The merchant processor must provide settlement capabilities for the full amount of valid transactions that are captured. These transactions will be batched and electronically deposited through Automated Clearing House (ACH).	Describe the settlement process of the merchant processor including how funds are batched and deposited via ACH.	Must Have
Pay Connexion supports e-check payments that are processed as ACH debit transactions. ACH transactions are processed through a separate clearing network in batch process, per NACHA guidelines. e-checks/ACH debits			

are a popular, low-cost electronic payment alternative to payment cards. Pay Connexion supports the acceptance of all consumer and business e-check payments, processed through ACH.

All e-check/ACH payments are made in compliance with NACHA and applicable regulatory requirements. Among the NACHA requirements that Pay Connexion supports is that the City employ commercially reasonable measures to minimize the potential for fraud. Pay Connexion assists the City in meeting these requirements through the use of a shared secret, called 'Payer ID', that is determined during implementation. This value can be passed to Pay Connexion in the session transfer, or via a pre-registration file, if used.

Settlement processing and timing is in accordance with the standard timeframes as indicated below for supported payment vehicles.

- If supported in the Biller's configuration, all e-check payments are processed as ACH debit transactions by J.P. Morgan. All transactions are processed and settled in batch.
- All credit and debit card payments are processed by Chase Paymentech Solutions. Authorization takes place in real-time and are settled in batch.

If ACH/e-check e-payments are supported in the City's configuration, these transactions will be processed as ACH debits originated by J.P. Morgan on behalf of the City through J.P. Morgan's ACH processing platforms. All ACH/e-check payments made each business day before 9:00 PM ET will be processed in a batch and presented for processing. The Pay Connexion system will debit funds from the customer's account via ACH and credit the City's DDA. Funds will settle on the next business day (excluding weekends and Federal Reserve holidays) to the City's DDA at J.P. Morgan.

Payment Settlement for Card transactions varies depending upon which platform the client is on. There are two platforms: Global and North American.

Below is the typical settlement timing for e-payment transactions; however, the City has flexibility to choose different cut-off times.

Table 5 - Global Card Platform Cut-Offs

Payment Completed	ACH/ e-check Payment (9 pm ET Cut-Off)	Credit/Debit Card Transactions Authorized Through Chase Paymentech – Global Card Platform		
		Card Transactions (Day of Batch Closed)	Day Paid via ACH for Transactions	
			Visa, MasterCard & Discover* and ATM Cards (Star, Nyce, Pulse)	American Express
Monday	Tuesday	Monday 8 pm EST	Wednesday	Friday
Tuesday	Wednesday	Tuesday 8 pm EST	Thursday	Monday
Wednesday	Thursday	Wednesday 8 pm EST	Friday	Tuesday
Thursday	Friday	Thursday 8 pm EST	Monday	Wednesday
Friday	Monday	Friday 8 pm EST	Tuesday	Thursday
Saturday	Tuesday	Saturday 8 pm EST	Wednesday	Thursday
Sunday	Tuesday	Sunday 8 pm EST	Wednesday	Thursday

Table 6 - North America Card Platform Cut-Offs

Payment Completed	ACH/ e-check Payment (9 pm ET Cut-Off)	Credit/Debit Card Transactions Authorized Through Chase Paymentech – North America Card Platform		
		Card Transactions (Day of Batch Closed)	Day Paid via ACH for Transactions	
			Visa, MasterCard & Discover	American Express
Monday	Tuesday	Tuesday 5 am EST	Wednesday	Friday
Tuesday	Wednesday	Wednesday 5 am EST	Thursday	Monday
Wednesday	Thursday	Thursday 5 am EST	Friday	Tuesday
Thursday	Friday	Friday 5 am EST	Monday	Wednesday
Friday	Monday	Saturday 5 am EST	Tuesday	Thursday
Saturday	Tuesday	Sunday 5 am EST	Wednesday	Thursday
Sunday	Tuesday	Monday 5 am EST	Wednesday	Thursday

Please note that American Express payments are not supported under the Convenience Fee model at this time.

F211	**PCI-DSS (Level 1) Compliance:** The merchant processor must be PCI-DSS (Level 1) compliant	Provide the system PCI-DSS (Level 1) documentation.	Must Have

Pay Connexion is listed with PCI-DSS as compliant (Level I), receiving a favorable rating from the assessor during the March 31, 2012 audit. Included in the PCI-DSS review is establishing and maintaining a secure network, protection of card holder information, data access and controls, and regular system and network monitoring.

Proof of PCI-DSS Compliance can be found at:

Visa: http://usa.visa.com/download/merchants/cisp-list-of-pcidss-compliant-service-providers.pdf
Search on "Pay Connexion"

MasterCard: http://www.mastercard.com/us/company/en/docs/SP_Post_List_2012.pdf
Search on "PayConnexion"

F212	**Credit/Debit Merchant ID Reference:** The merchant processor must reference the merchant ID for all ACH credits and debits. All electronic credits and debits shall be separated by Merchant ID.	Explain how the merchant processor references and separates both credits and debits by merchant ID.	Must Have

Please see our response to *Req #F120* above.

Additionally, for any specific Merchant ID / Company ID, the DDA utilized for settlement of payment batch deposits may be designated separately from the DDA utilized for Chargebacks (card) or returns (ACH).

F213	**Deposit of Credit and Debit Sales:** The	Describe the process your system uses to	Must

merchant processor must deposit all funds received from credit and debit card sales to an account at a financial institution designated by the City.	deposit funds received from credit and debit card sales into a designated account in a financial institution.	Have

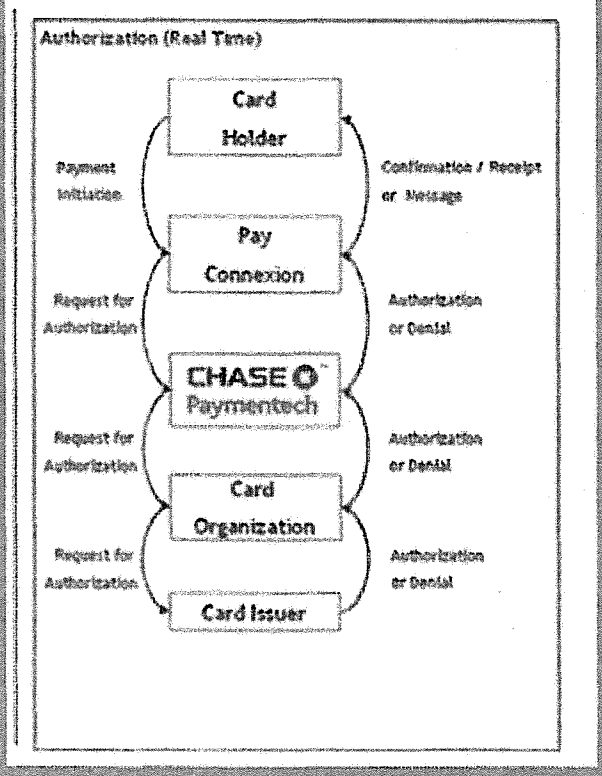
Transactions will be sent to Chase Paymentech's Authorization Transaction Database. During data validation and authorization, transactions are routed to the card issuing databases at the appropriate card organization (e.g., Visa, MasterCard). After authorization is complete, the settlement process begins in accordance with applicable rules, regulations and timelines. Customers will be notified if the card payment does not pass a series of validation and verification checks, including various card number validations, address verification service (AVS), card verification data (CVD) and authorization attempt limits, or if the card payment is not authorized by the merchant processor. Payment will only be confirmed when the validations and authorizations have occurred successfully. J.P. Morgan will retain credit card authorization logs and transaction records as required by applicable law and the rules, regulations, and operating procedures of the respective card organizations.

J.P. Morgan is responsible for capturing and validating the following information:

- The payment amount is less than or equal to the Total Amount Due
- The credit card or debit card number is checked and validated to meet with card organization rules
- The proper credit card expiration date matches with the card issuing database
- The name and address of card holder matches with the card issuing database
- Telephone number exists and is a required field
- The e-mail address is a required field and is a valid format

Pay Connexion supports the real-time authorization and batch settlement of credit card and debit card transactions. Pay Connexion processes credit/debit card transactions in coordination with the merchant processor (Chase Paymentech), the card organizations (e.g., associations/networks), and card issuers.

Processing: Credit/Debit Cards



Each day's transactions, including adjustments, such as refunds and returns, are reflected in the daily remittance file. Additionally, the Payment Card Batch Report is available via the administrative site and is useful in reconciliation of card payments.

F214	**Debiting of Merchant Processing Fees:** The merchant processor must have the capability to debit the City for any and all merchant processing fees assessed to the City according to individual Merchant ID via ACH. The City will designate the account to be debited.	Describe the processes your system supports for debiting merchant processor fees.	Must Have

Pay Connexion supports two separate funding models, either of which may be selected on a Biller (i.e., City Department basis) during the Configuration Requirements Definition phase of implementation.

City Funded Fee Model

Through a City Funded fee model, fees for the application are passed on to the City. Typical City Funded costs include setup (implementation), monthly hosting, and per transaction fees paid by your organization for the application. Additionally, the City pays the related credit card discount fees/interchange and merchant processing fees. Under this model, the card processing fees are debited from the City's designated DDA for each Merchant ID as defined during the Configuration Requirements Definition phase of implementation.

Convenience Fee Model

Pay Connexion supports many convenience fee structures, such as percentage, tiered, or flat fee. With a convenience fee model, a fee is passed on to the payer using the e-Payment application. The convenience fee option is a no-cost convenience fee model, where the City pays no fees. J.P. Morgan collects a convenience fee from the payer. J.P. Morgan pays all fees associated with the transaction, including interchange, dues, assessments, and merchant processing fees. In this model, the City does not pay implementation, hosting, or per transaction fees.

F215	**Supported Card Types:** The merchant processor must process Visa and MasterCard credit and debit cards. It shall also process other card types (e.g. American Express and Discover).	Describe the type of cards your system can process.	Must Have

Please see our response to *Req #F210* above.

Through Pay Connexion, we can accept all major credit and signature debit cards: Visa, MasterCard, Discover and American Express (including procurement cards, gift cards, pre-paid cards). Pay Connexion can also support the use of ATM cards with NYCE, STAR, and PULSE logos. Pay Connexion supports e-check payments (processed as ACH debits). Please note that Pay Connexion does not support American Express payments under the convenience fee model at this time.

F205	**Fund Transfer Timeframe:** The merchant processor should transfer electronic funds to the City within two business days of receipt.	Describe the turnaround time for fund transfers to the City.	Expected

Please see our response to *Req #F210* above

F216	**Merchant Processor Headquarters:** The merchant processor should be headquartered and process transactions in the United States.	Describe where the merchant processor is headquartered and where they process transactions.	Expected

Chase Paymentech's Headquarters are located at 14221 Dallas Parkway, Building Two, Dallas, TX 75254.

Due to the sensitive nature of this information, J.P. Morgan does not release specific details on the location of primary and backup data centers and processing sites.

All backup sites and hot-site locations are in a separate zone or region depending on the product and regulatory requirements of the country in which we are operating. J.P. Morgan's corporate policies use the zone designation to measure and depict local diversification of infrastructure and access.

To address wide-scale disruption, the term region, as a designation, is used to measure and depict the susceptibility of multiple locations to the same wide-scale disruption. An analysis to determine zone and region designation is performed by our Corporate Real Estate/Corporate Security/Global Life Safety business units with input from Corporate Technology and Corporate Resiliency Risk Management.

F217	**Minimum Merchant Processing History:** The merchant processor should have an ongoing minimum of five years of experience processing credit and debit transactions.	Describe the amount of ongoing experience the merchant processor has processing credit and debit transactions.	Expected

Since 1985, Chase Paymentech has provided services to merchants across a range of industries and segments by managing costs, mitigating risks and opening new lines of potential revenue. Our unique combination of

service and solutions has placed us at the forefront of the payments industry – supporting new endeavors, exploring new avenues of commerce and using our technology to provide safe, reliable payments to our merchants.

With more than 25 years of experience, our longevity and stability make us a recognizable name in the payments industry, while the strength of our ownership gives you a solid foundation to both establish and grow your business.

F218	**Transaction Processing Expectation:** The merchant processor should process all transactions submitted by the City that are valid, and satisfy applicable rules, regulations and laws.	Describe any conditions or obstacles that may potentially block transactions from being processed.	Expected

Please see our response to *Req #F526* above.

F219	**Electronic Authorization/Capture Availability:** The merchant processor should provide electronic authorization and capture capability for transactions 24 hours a day, 7 days per week.	Describe the availability of the system to provide electronic authorization and capture capability.	Expected

J.P. Morgan monitors Pay Connexion system availability and performance through human and automated means. Performance issues trigger alarms that are escalated through our Information Technology Operations Support (ITOS) group for prompt resolution. Further, performance is reviewed weekly with our senior management team. If Pay Connexion consistently reaches 60 percent utilization, we augment the platform with the necessary hardware and software components.

The Pay Connexion Service Level Agreement availability commitment is that the service will be available 99.5% of total minutes in each month, excluding planned outages. Planned outages are taken as needed for purposes such as the release of new functionality and other maintenance. In the event of a planned outage, notice is given at least 24 hours in advance of the scheduled outage. Downtime is scheduled within a standard window of Sunday 1:00 a.m. to 7:00 a.m. ET. Other planned outages, if necessary, are performed with notice. Historically, J.P. Morgan has managed availability well in excess of our 99.5% SLA commitment, as evidenced by the following statistics:

Table 7 - Pay Connexion Service Availability

Availability	2006	2007	2008	2009	2010	2011
Web	99.82%	99.67%	99.89%	100.00%	99.78%	99.96%
Admin Site	99.56%	99.67%	99.88%	100.00%	99.9%	99.96%
IVR	99.79%	99.60%	99.74%	100.00%	99.9%	99.96%

F220	**Regulated Chargeback Process:** The merchant processor should process all chargebacks in accordance with the applicable card regulations governing chargebacks.	Describe how chargebacks are processed in accordance with applicable card regulations.	Expected

The Chase Paymentech Chargeback Department will work with the City to evaluate every disputed charge. If Chase Paymentech is unable to remedy the chargeback, we send it to you with all supporting documentation. You may then research the transaction for a possible remedy. Included in each chargeback package is a merchant recourse form, which outlines the nature of the chargeback and the information required to reverse it. Chase Paymentech's chargeback support will ensure that this impact is minimized.

Chargeback retrievals are a request for information from the issuing bank. They are typically initiated upon a cardholder's request. If the cardholder does not recognize a charge on their billing statement, they may contact their bank and request further information. This is done as a Chargeback Retrieval Request. Chase Paymentech receives retrieval requests electronically as part of their daily incoming chargeback files. They are matched against the Order History Database and a facsimile draft is produced which is either mailed or imaged to the initiating issuing bank.

Chargeback retrieval requests are also delivered to the merchant in order to obtain the required proof of the transaction. The printed proof of the transaction is then attached to the document and forwarded to the issuer. According to Visa and MasterCard Operating Regulations, an acquirer (i.e., Chase Paymentech) has 30 calendar days from the date received to fulfill a chargeback retrieval request (also referred to as a "request for copy"). Merchants are given until day 16 of the 30-day lifecycle to fulfill ticket retrieval requests. If a request is unfulfilled as of day 14, Chase Paymentech will send a second request via fax, provided that the merchant is set up for fax delivery of their retrieval request notifications.

Generally, if a retrieval request is not fulfilled (i.e., copy of receipt is not presented), the retrieval becomes a chargeback. Facsimile and scanned images are acceptable means of producing the requested drafts.

Chase Paymentech ensures that operating procedures for exception processing, including retrievals and chargebacks, minimize City impact while addressing cardholder issues. Chase Paymentech's processing rules are written to generate a retrieval or chargeback response without City involvement if the required information is accessible by Chase Paymentech.

Customer support will be handled by the Operations Practice Management (OPM) team. OPM is available to support the City 24/7/365 via a toll free phone number. OPM will work with Chase Paymentech to designate a Chargeback Analyst to assist with your account. Your designated Chargeback Analyst will be the single point of contact for all chargeback issues (with additional assistance from your Account Executive). Your Chargeback Analyst will review every chargeback for proper documentation and adherence to the payment brands' rules and regulations. All items are addressed and processed within the required time frames to ensure that your re-presentment rights are fully preserved.

F221	**Reporting Requirements:** The merchant processor should enable the daily access and printing of various types of reports.	Describe the reporting capabilities of the merchant processor including what fields can be included.	Expected

Authorized City administrators access the Pay Connexion administrative site from a standard web browser. The administrative site provides authorized City personnel with the ability to make payments, execute refunds (refund rules differ by payment method), generate a wide range of reports on demand, and perform other administrative functions.

Authorized personnel access the administrative site through a secure URL. Each session is secured using Secure Sockets Layer (SSL) with 128-bit encryption technology. Authentication is required for customer service representatives and administrators to access to the administrative site. All data is stored securely. This easy yet secure access to transaction and other information is ideal for efficient customer support and issue resolution. In addition, an online context sensitive 'Help' utility is available to administrative users.

Transaction history is saved for 24 months (2 years) online, and an additional 5 years offline. By law, we are required to save this information for 7 years.

Authorized City administrators access the Pay Connexion administrative site from a standard web browser. The administrative site provides authorized City personnel with the ability to make payments, execute refunds (refund rules differ by payment method), generate a wide range of reports on demand, and perform other administrative functions.

Single Payments Section
- View Pending Payments
- View Payment History
- View Payment Details
- Make User Payment
- Refund Payment
- Cancel Pending Payment
- Edit Pending Payment
- Reactivate Payer for ACH Payments

Recurring Payments Section
- Make User Recurring Payment
- View Recurring Payments
- View Recurring Payment Details
- Edit Recurring Payment
- Stop Recurring Payment

Registered Payers Section
- Reset Registered Payer Password
- View Payer Profile
- Edit Payer Profile

Payment Accounts Section
- View Payment Account
- Delete Payment Account
- Enable Invalid Account

Customer Service Section
- Initiate Call (all customer service functions accessed through Initiate Call)

Administrative Reports Section
- Payment Detail Reports
- Payment Summary Reports
- Download Remittance File
- Download CSR Payment Reports
- Card Batch Reports
- Recurring Payment Reports
- Admin User Access Report
- Fraud Detection Report

Figure 12. Pay Administration Site Main Menu

Please see *Attachment 2* for sample Pay Connexion reports.

F222	**Merchant ID Statement Reports:** Individual merchant ID reports should be provided monthly for transactions processed and fees charged to the City for the previous month.	Minimum contents of the monthly statement reporting to include detailed transaction description, name of brand card, amount of transactions, transaction fee amount and detail concerning calculation of the transaction fee amount (e.g., interchange type assigned).	Expected

In addition to monthly statements that can be received via e-mail or on-line, Chase Paymentech offers a full array of Internet-based processing reports through Resource Online, its proprietary suite of innovative Web-based tools that enables merchants to quickly and easily access their payment processing data. Resource Online provides access to front-end point-of-sale data, back-end reconciliation data, and more. Access is modular, so we can tailor your needs to the tools that make the most sense for your business.

Regardless of your needs, Resource Online offers the following features and benefits:

- Cost Savings – View and analyze payment data quickly and efficiently
- Improved Cash Flow – Review deposit activity daily
- Time Savings – Review data quickly with 24/7 access
- Fraud Tools – Take advantage of tools and reports that can help identify fraudulent activity
- Secure access with optional card masking
- Variety of reports – Summary, detail and trending reports allow you to effectively manage your payment processing data
- Customize how you view your data with user preferences and filters
- View, print, save or export your data for further analysis
- Easy to learn, with online help just a click away
- Comm Central - Increases operational efficiency by putting an array of payments information at your

fingertips and streamlines communication processes by providing one central resource for most external information

The modules of Resource Online provide access to reports that can be generated on a daily, weekly and monthly basis and include financial and transaction detail, retrievals and chargebacks, and customized analytical summaries. Internet access and a Web browser are the only prerequisites for access. You can select from a broad variety of standard reports to suit your documentation needs. Together with your designated Account Executive, you can also design customized reports to meet the special needs of your organization.

Each module within the Resource Online suite offers a variety of transaction and portfolio-based information. Resource Online's modules include:

- Virtual Transaction Manager
- Recon Solution, and the optional modules:
  - Decisionable Data
  - Respond
- Instant Alerts

Resource Online also includes standard features available to all subscribers, including:

- **Admin** – Create additional users, change report access or delete users
- **Bank Lookup** – Search for card issuing information to assist in research
- **File Download** – Receive data files, if applicable
- **Merchant Search** – Search for locations within your hierarchy using various search criteria

Virtual Transaction Module:

Virtual Transaction Manager (VTM) provides 24/7 real-time access to a merchant's front-end point-of-sale, batch and transaction data, allowing transactions to be viewed seconds after they have occurred. VTM offers summary and detail reports, as well as the ability to search for transactions that meet certain search criteria. Merchants can select criteria such as viewing data at a merchant or hierarchy level, specify date ranges, and other applicable criteria, and view results at the click of their mouse.

Available reports include:

- Batch Summary
  - Batch detail
  - Transaction detail
- Card Type Summary
- All Transactions
- Transaction Search
- Suspense Batch Summary

Recon Solution Module:

Recon Solution provides access to comprehensive reports to support your reconciliation, research and analytical needs. With a few clicks of the mouse, the merchant can view deposits, batch activity, transaction detail, card totals, qualification information, funding data, processing fees, adjustments, retrievals and chargebacks, authorization detail, and statements online.

The available reports include:

- Recap Summary
- Exceptions Summary

- Batch Summary
- Batch Exception
- All Transactions
- Card Type Summary
- Card Type Summary by Merchant
- Private Label
- Settlement Summary Select
- Settlement Fees Summary
- Settlement Fees Detail
- Summary of Fees
- Deposit Rejection
- Financial Adjustments
- Card Number Search
- Card Number History
- Authorization Search
- Qualification Search
- Non-Qualified Transactions
- Qualified Transactions
- Dispositions
- Reversals
- Denied Reversals
- Representments
- Debit Adjustments
- Outstanding Retrievals
- Expired Retrievals
- Fulfilled Retrievals
- Statements
- Hierarchy Structure
- Location Search
- Card Type Analysis
- Debit Card Analysis
- Debit Monthly Card Analysis
- Deposit Rejection Analysis
- Dispositions Analysis
- Reversals Analysis

Recon Solution Optional Modules:

- **Decisionable Data** – Chase Paymentech has identified three areas that should be monitored on a regular basis to ensure their organization is operating as efficiently as possible when it comes to payment processing. These areas are Credits Without Offsetting Debits, Transaction Qualification, and Chargebacks and Retrievals. These innovative reports highlight locations that may not be running as efficiently as possible, or may be experiencing fraud and ultimately costing your organization more money. Our Decisionable Data reports empower you to minimize losses, maximize profits and minimize interchange costs.
- **Chargeback Imaging System** - The interactive Chargeback Management module of Resource Online enables merchants to manage exception items such as chargebacks and retrievals online. Merchant users can view and immediately respond to inquiries via the Internet, dispute or accept chargebacks, and fulfill retrieval requests. Merchants can respond to Chase Paymentech using a text message, a scanned sales receipt or other documentation, or a combination of both.

Instant Alerts Module:

Instant Alerts automatically and instantaneously notifies a user of potential financial risks and exception conditions that Chase Paymentech detects while reviewing the merchant's payment processing data. Alerts are generated according to thresholds you set and can change when necessary, thereby allowing you to determine what, how and when you receive your alerts. The user is notified via email when one of the locations meets or exceeds a specified threshold in the following categories: Chargebacks, Retrievals, Interchange Qualification and Velocity. Instant Alerts can proactively keep you on the forefront of your financial operations and allow you to focus on what you do best—running your business.

Please see *Attachment 3* for a sample monthly merchant statement and *Attachment 4* for a sampling of Resource Online reports.

TECHNICAL REQUIREMENTS

To ensure that a proposed solution is thoroughly represented, Vendors must respond to each requirement listed below. The three "Importance Levels" are:

Must Have: These requirements may or may not be industry standards but are highly critical to the project. They must either be satisfied by the system's base functionality or the Vendor must offer an alternative such as customization.

Expected: These requirements are important to the end users of the system and generally are features that are industry standards. The majority of these requirements need to be satisfied.

Desired: These requirements add value, but are not critical to end users. These features are considered optional.

If there are requirements that are not applicable to your proposed solution, please mark those items "N/A" and provide a brief explanation as to why this in not applicable.

Application Software Requirements

Req#	Requirement Description	Required Response	Rating
T1.1.5	**Technical Architecture Documentation:** The vendor should provide documentation depicting the technical architecture of the components of their system, including a simple network architecture diagram.	Provide system documentation and a simple diagram of the proposed solution architecture that shows the hardware components and indicates the types of data exchange between components.	Expected

J.P. Morgan will provide a redundant transaction processing system to backup the primary transaction processing system. Both will be supported by necessary contingency planning to ensure that disaster recovery processes will support transaction processing in the event of a disruption affecting the primary system. In the event of a failure of the primary transaction processing system, the backup system will be deployed within one hour of the primary system outage.

J.P. Morgan operates its highly available, fully-hosted Pay Connexion solution at two geographically dispersed data centers, a primary and a "hot" backup. The equipment located at the backup data center mirrors that at the primary data center in sizing and configuration. At each tier, (i.e., Web, Application and Database), the components of Pay Connexion are configured identically at each data center. In the event of an emergency or disaster, recovery operations simply involve switching the networking components from the primary data center to the backup data center. Normal business operations can then resume at the backup data center within the stated service level agreements.

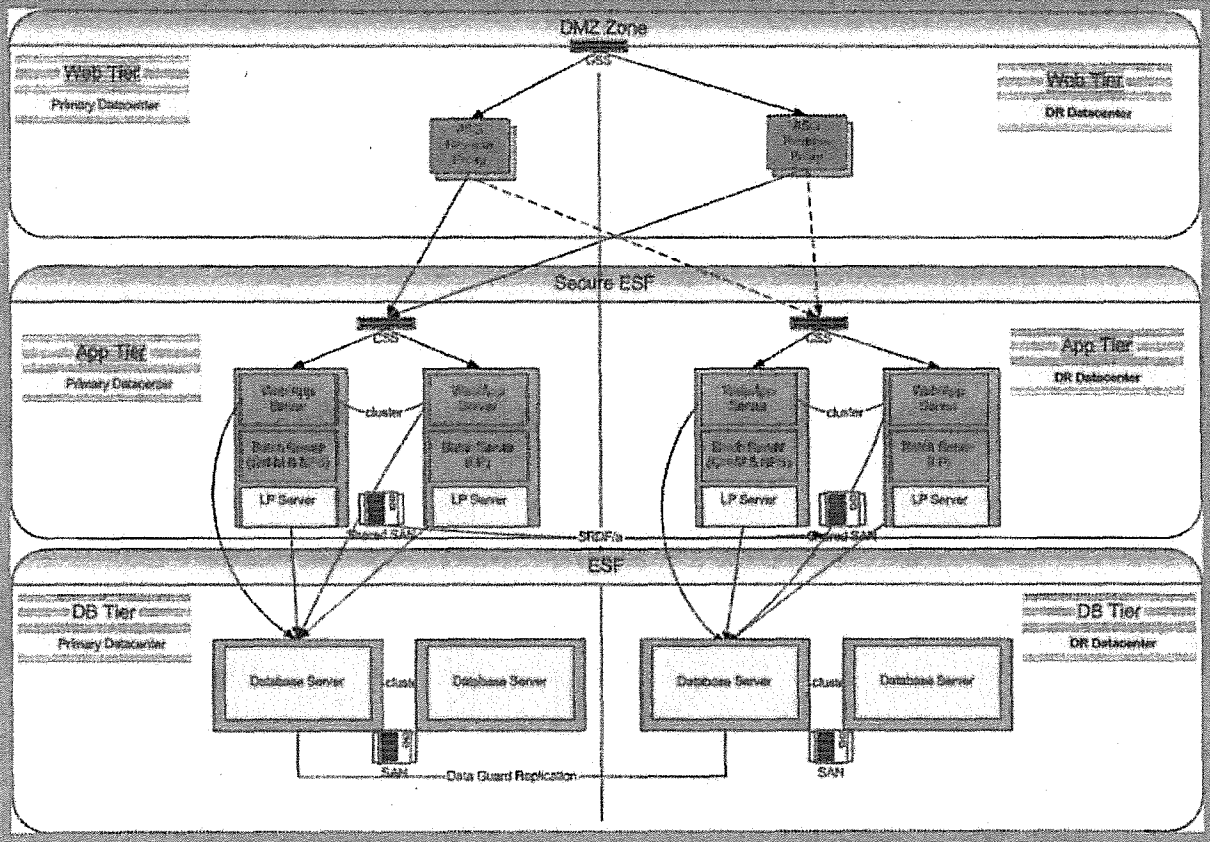
Each J.P. Morgan business unit performs a formal business impact analysis to assess the operational, financial and reputation impact of a service disruption on clients and the firm. The results of the business impact analysis are used to determine the criticality of the function and the corresponding recovery time objective.

Recovery time objectives and service levels vary based on criticality of the specific business function. For our most critical functions, we apply a two-hour recovery time objective for full resumption of normal operations. For the least critical functions, we apply a recovery time objective of 73 hours, which results in those business functions deferred and/or suspended.

Business and support group areas must identify their requirements based on their process capacity needs to address a loss of an entire zone for a minimum of 30 days. This enables businesses and support groups to stage their recoverability over that time period.

We conduct a live cutover to our backup processing site for a full 24 hours. This process helps to validate that all components are tested each year providing a high level of confidence that we can move to our backup site, if needed. All test results and business continuity plans are reviewed by our internal auditors and as part of an annual independent operational audit.

The diagram below illustrates Pay Connexion's operating environment.



Pay Connexion's operating environment offers several disaster recovery protections:

- Data Centers
  - Two Geographically Dispersed Data Centers: Primary and DR
  - Virtual Servers shared with Pay Connexion
  - Shared IVR infrastructure with Pay Connexion
  - Shared DR/UAT environment
- Hardware Architecture
  - SSL offload
  - Dual active web server
  - Dual active application server
  - Clustered active/standby database server
  - DR database servers replicated

T1.1.8	**Desktop Component Compatibility:** The proposed solution's client interface (whether client software or web browser) should maintain compatibility with routinely updated desktop components.	Describe how your software developers maintain standard desktop components including interim browser updates, Java and JavaScript updates, Windows OS security patches, Flash, Firefox, IE, Adobe Reader, etc.	Expected
Pay Connexion supports Microsoft Internet Explorer version 6.0, 7.0, 8.0 or Firefox 3.0, 3.5 or Google Chrome 3.0. Also, browsers must be enabled for both Java Script and Cookies. In applications configured for electronic statement image presentment, Pay Connexion includes a link from which payers may download Adobe Reader (if needed) for viewing *.pdf images of their bills.			
T1.1.1	**Operating System Compatibility:** The desktop component of the solution should be able to run on MS XP and Windows 7 Operating Systems (City desktops are managed via the network).	Describe what operating environment is compatible with the system.	Expected
Pay Connexion is able to run on MS XP and Windows 7 Operating Systems, so long as a supported web browser is used. Both Pay Connexion's Web channel and admin site are browser-based. There is no client application to install on any PC to use the system. Pay Connexion supports Microsoft Internet Explorer version 6.0, 7.0, 8.0 or Firefox 3.0, 3.5 or Google Chrome 3.0 or Safari 4 or 5. Also, browsers must be enabled for both Java Script and Cookies. In applications configured for electronic statement image presentment, Pay Connexion includes a link from which payers may download Adobe Reader (if needed) for viewing *.pdf images of their bills.			
T1.1.3	**Third-Party Vendor Identification:** The vendor should identify any third-party software products used within the proposed system configuration.	List any third-party software products used within the proposed configuration. Include third-party DB management products, report/query tools, client-side products required. Also list any third-party tools supported, but not provided (i.e. report writing)	Expected
J.P. Morgan's comprehensive solution is held under "one roof". Not only is development, sales, implementation and support of our product performed by J.P. Morgan, so, too, is the processing of both credit/debit card and ACH/e-check payments. Chase Paymentech is the nation's leading merchant processor, and J.P. Morgan has been the nation's highest volume ACH processor since the inception of NACHA. This provides you with a single point of accountability, and one that is worthy of your business. Chase Paymentech does not use a third-party to process transactions. We are a merchant acquirer and manage direct links to all of the Card Associations, as well as several private label credit card organizations. JPMorgan Chase, our parent company, is our sponsoring bank and is a full member of both Visa and MasterCard. Our processing facilities operate through JPMorgan Chase's specific Bank Identification Number assigned by Visa and Interbank Card Association numbers assigned by MasterCard. Since we have direct links to Visa and MasterCard, we settle transactions directly to the Card Associations without any intermediaries. Chase Paymentech also maintains direct connections to the major Debit Networks. This allows us to work directly with each entity within the realms of authorizations, funding, reporting, and transaction reconciliation. There are secondary market debit networks that outsource their transaction processing, and we connect to these as well. In a few cases, we access networks through these providers due to availability, which gives us additional demographic coverage. Chase Paymentech continuously analyzes these situations and will build a direct			

interface when conditions warrant.			
T1.1.7	**Supported Web Browsers:** If the application is web-based, the solution should support updated versions of Internet Explorer, Firefox and other client web browsers within 90 days of new releases of the browsers.	Describe how the system is tested and certified for compliance with new releases of Internet Explorer and Firefox web browsers. What other client web browsers are supported?	Expected
Both Pay Connexion's Web channel and admin site are browser-based. To use the Pay Connexion site, you will need Microsoft Internet Explorer version 6.0, 7.0, 8.0 or Firefox 3.0, 3.5 or Google Chrome 3.0 or Safari 4 or 5. Also, your browser must be enabled for both Java Script and Cookies. To use the web channel, the City is required to integrate code to support a web session transfer by which the payer is transferred to Pay Connexion to submit a payment. As with other functionality, Pay Connexion support of additional browsers/versions may be added via periodic product releases. There are typically three to five product feature releases annually, each of which includes functionality which is developed internally and tested extensively. Minor/Maintenance releases may also be deployed throughout the year. Prior to each major release, Release Notes will be delivered to the City's designated personnel outlining the features being deployed in the release.			
T1.1.9	**Development and Test Environment**: The solution should provide a development and test environment.	Describe the development environment provided by the system, especially with respect to developing and testing interfaces to other systems.	Expected
Following the Configuration Requirements Definition phase of implementation, each application is built according to City-defined requirements. The Build is provided to the City for User Acceptance Testing (UAT). The City will integrate its systems with this application as the City's functionality progresses from the City's Development environment to its Test environment to its Production environment. Each Build is in the Pay Connexion production environment, but remains in an "unlaunched" state until activated. Activation occurs only after the City as completed of UAT, signed-off on the approval to activate and after internal pre-activation due diligence is performed. Following activation, additional validations are performed prior to the City "opening" the payment channels to payers. To support testing after an application is has been activated, whether the testing is of City system changes or Pay Connexion configuration changes (e.g., associated with a Change Request project initiated to take advantage of new functionality introduced in a post-activation product release), a "Permanent Test Biller" application may be provided. This test application largely mirrors the production application, but isolates test activity from production activity. The City will integrate its systems with this application as the City's functionality progresses from the City's Development environment to its Test environment. When UAT in the Permanent Test Biller has been completed J.P. Morgan deploys any required configuration changes to the production application in coordination with City as needed given the specific scope of the change.			

Business Continuity Requirements

Req#	Requirement Description	Required Response	Rating
T1.3.5	**System Uptime:** The proposed solution must be capable of providing 99.9% uptime if the City chooses to require it. This level of	Explain how the solution can be designed to support this level of uptime. Indicate tools and methods supported by the	Must Have

availability may be directly supported by the proposed solution, or may use third-party tools and methods to achieve 99.9% uptime.	solution to provide the uptime requirement (such as hardware fault tolerance, clustering, mirroring, high availability platforms, etc.). Provide data for the past three years of service uptime.

Please see our response to *Req # T1.1.5* above.

The Pay Connexion Service Level Agreement (See the Pay Connexion Service Terms Agreement) availability commitment is that the service will be available 99.5% of total minutes in each month, excluding planned outages. Planned outages are taken as needed for purposes such as the release of new functionality and other maintenance. In the event of a planned outage, notice is given at least 24 hours in advance of the scheduled outage. Downtime is scheduled during a standard window at low use times. Other planned outages, if necessary, are performed with notice. Historically, J.P. Morgan has managed availability well in excess of our 99.5% SLA commitment, as evidenced by the following statistics:

Table 8 - Pay Connexion Availability by Payment Channel

Availability	2006	2007	2008	2009	2010	2011
Web	99.82%	99.67%	99.89%	100.00%	99.78%	99.96%
Admin Site	99.56%	99.67%	99.88%	100.00%	99.9%	99.96%
IVR	99.79%	99.60%	99.74%	100.00%	99.9%	99.96%

Table 9 - Pay Connexion Service Level Desciptions

Technology Service Level Description	Minimum Service Level Criteria
Web Availability / Uptime	Goal: Pay Connexion℠ Transaction System web applications will be available to users ninety-nine percent (99%) of the total minutes available in each month. Availability is calculated excluding any Scheduled Maintenance or scheduled System Outages. In addition, there shall be no more than two (2) System Outages (planned or unplanned) during each twenty-four (24) hour period (measured from midnight to midnight), and the aggregate time of the System Outages during that period shall not exceed two (2) hours.
IVR Availability / Uptime	Goal: Pay Connexion Transaction System IVR applications will be available to users ninety-nine percent (99%) of the total minutes available in each month. Availability is calculated excluding any Scheduled Maintenance or scheduled System Outages. In addition, there shall be no more than two (2) System Outages during each twenty-four (24) hour period (measured from midnight to midnight), and the aggregate time of the System Outages during that period shall not exceed two (2) hours.

	Web and IVR Disaster Recovery	Provide an offsite hot backup site. Primary processing capabilities will be available within 8 hours if primary site is disabled.	
	Web and IVR Backup Recovery Testing	The backup recovery systems to be tested annually.	
	Standard Pre-Registration File Processing	Billers with the Pre-Registration feature are required to deliver a Pre-registration file to the Pay Connexion team by 9pm Eastern time in accordance with their daily delivery schedule. Pay Connexion will process the Pre-registration file upon receipt from the biller or an intermediary. Response files will be delivered to the biller by 9AM Eastern time, in accordance with the Biller's daily delivery schedule. If the Biller does not deliver a Pre-registration file on time the Pay Connexion team will make best efforts to meet the 9AM delivery Response file but will not guarantee a 9AM delivery time.	
	Standard Next Day Remittance File Processing	The Pay Connexion team will deliver a Remittance file to the Biller (either directly or through an intermediary) by an agreed upon time, Monday through Friday, excluding Federal Reserve holidays.	
	Standard Same Day Remittance File Processing	The Pay Connexion team will deliver a Remittance file to the Biller (either directly or through an intermediary) by an agreed upon time, Monday through Friday, excluding Federal Reserve holidays.	
T3.3.2	**Disaster Recovery:** The system must protect data in the event of system failure.	Describe how system protects data in case of system failure. Include a discussion of the backup procedures used to meet this requirement.	Must Have

J.P. Morgan operates Pay Connexion at two data centers: a primary and a "hot" backup. The Pay Connexion environment is hosted in geographically dispersed regions. The equipment located at the backup data center mirrors the primary data center in sizing and configuration. At each tier, (i.e. Web, Application, and Database), the components of Pay Connexion are configured identically at each data center. In the event of an emergency or disaster, recovery operations simply involve switching the networking components from the primary data center to the backup data center. Normal business operations can then resume at the backup data center within the stated service level agreements. The backup environment can be made available within 8 hours. Other than for testing purposes, our backup environment has never been required.

We have outstanding system availability, as evidenced by the following details of our 2009 performance against the availability targets of the Pay Connexion public and administrative websites:

- Minimum Acceptable Performance (MAP) per SLA: 99.50%
- Actual performance: 100.00%

J.P. Morgan monitors system availability and performance through human and automated means. Performance issues trigger alarms that are escalated through our IT Operations Support area for prompt resolution. Further, the performance is reviewed weekly with our senior management team. If our system consistently reaches 60 percent utilization, we augment the platform with the necessary hardware and software components.

We place a high priority on the ability to proactively contact you in the event of transmission problems. Our Operations staff monitors the processing of all merchant files and is notified of any failed files so that they can identify the cause. The Operations staff investigating the failure contacts you immediately to explain the situation and to discuss what action needs to be taken. Back-ups, archives, disk space usage, and CPU usage are all part of Operations' daily functions. Any area that falls below 100 percent for that day's performance level becomes an immediate priority to investigate and resolve. Not until an issue is completely resolved is it removed as a top

priority.			
T3.3.3	**System Maintenance:** The system should follow a predefined maintenance schedule. The city will negotiate regular maintenance periods outside of this requirement.	Describe how the vendor handles regularly scheduled maintenance.	Expected

PLANNED / SCHEDULED OUTAGES

In the event of any planned or scheduled System Outages, it is expected that Bank will contact the appropriate individuals designated by Customer at least twenty-four (24) hours prior to the planned System Outage (contact information will be amended from time to time via e-mail). Additionally, in the event of a planned / scheduled System Outage, it is expected that Bank will adhere to the following guidelines:

1. Downtime will be scheduled during standard maintenance windows of Saturday and Sunday 01:00 AM – 07:00 AM Eastern Time (ET), except as necessary and upon notice as provided above.
2. Bank will implement a web page on the payer site notifying that the system is unavailable during the scheduled downtime (Bank will immediately remove this notification page following completion of the scheduled maintenance).
3. Bank will implement a message on the IVR notifying that the system is unavailable during the scheduled downtime. (Bank will immediately remove this message following completion of the scheduled maintenance).

UNPLANNED / UNSCHEDULED OUTAGES

J.P. Morgan adheres to the following Severity Level-based approach to unscheduled Pay Connexion System Outage/service interruptions notification. The City is able to designate which individuals are to receive notifications. The City will be given a written notification of breach of a service level.

Table 10 - Pay Connexion Outage Notifications

Severity Level Definition	Initial Contact w/ Clients / Internal Functional Teams
Primary Definition: Severity 1 (Emergency) – Degeneration in or complete failure of, the system or any single channel (Web, Admin) to receive and process payments. Restricted to true, system-wide emergencies. A complete failure has occurred in either a system or critical process.	15 min to Client contacts and/or Internal Functional Team Designate (TBD); hourly updates until resolved
Primary Definition: Severity 2 (High) – Degeneration in, or complete failure of, business-critical secondary functionality (RTPC, all file processing, password reset, download a Remittance File, or the ability to initiate a call) for a single Biller or group of Billers Used when the problem is severely affecting a group of users. A major portion of a system or process is not functional, but can be bypassed, or it is a functional failure with no workaround.	15 min to Client contacts and/or Internal Functional Team designate (TBD); hourly updates until resolved
Primary Definition: Severity 3 (Medium) – Degeneration in product functionality of non-critical tertiary functionality (confirmation emails, standard reporting, etc) for a single Biller or a group of Billers This is the most common severity level. A system or process is mostly functional but not performing as expected. An error can be ignored, or a workaround can be used.	Monthly issues logs
Primary Definition: Severity 4 (Low) – System or critical process is functional, but a problem exists related to ease of use (slow app response time or screen flows), interface or Standard Report content, or a problem exists for a single Payer or group of Payers (can't reset passwords, can't log in). A single Payer is impacted. A system or process is currently fully functional, but a problem exists or the problem relates to	Monthly issues logs

	information, process change(s), minor enhancement(s), or request(s) for future functionality.		
T1.3.1	**Data Archiving:** The solution should enable data storage and retrieval from archived data. Data Archiving mechanisms shall include configuration and metadata elements as part of their capability.	Describe how the application is restored from a backup, and the user environment and the data environment are reestablished, verified and confirmed. What are ALL the steps required?	Expected
Please see our response to *Req T1.1.5* above. Transaction history is saved for 24 months (2 years) online, and an additional 5 years offline. By law, we are required to save this information for 7 years.			
T1.3.2	**Data Archiving Dataset Definition:** The solution should allow a user with appropriate privileges to define datasets to be archived, retention periods for current and archived data, and the date and time of archival.	Describe the solution's data archiving solution. Indicate how appropriate users can define datasets to be archived, retention periods for current and archived data, and the date and time of archival. Describe all other user-definable features.	Expected
Transaction history is saved for 24 months (2 years) online, and an additional 5 years offline. By law, we are required to save this information for 7 years. Statement Images are retained online for 18 months. Archived information may be accessed by request to the Client Service / Operations Practice Management team.			
T1.3.6	**Data Recovery:** The solution should be able to recover specific data records and/or files from backup and/or near-line storage.	Explain how certain selected records and/or files can be recovered from backup data and made available to the application.	Expected
Please see our response to *Req T1.3.2* above.			
T1.3.7	**Solution Scalability:** The solution should be scalable for future growth.	Provide the number of concurrent users the proposed system can support, and explain the software and hardware changes required to allow growth. Include the licensing structure and the cost levels.	Expected
The proven Pay Connexion platform is being used today by other clients to process over 19 million annual transactions totaling over $64 billion. The Pay Connexion IT department regularly performs system capacity planning and analysis of future growth. Currently, the Pay Connexion environment is adequately architected (server size, disk space, etc.) to handle the current volumes as well as projected growth. Additional Storage Area Network (SAN) is forecasted and SAN allocation is monitored regularly to ensure we have adequate space to accommodate future growth. As we add volume, we expect the system to continue to scale. As a general rule, we move to increase capacity once we transaction volume reaches 60% of available capacity.			
T1.3.8	**Suspended Transaction Resolution:** The system should allow authorized users to control and correct suspended or aborted transactions caused by an unexpected system, network or workstation outage.	Describe how the application administrator can correct suspended or interrupted transactions (i.e. ACID Test Compliance).	Expected

In the event that any transactions are suspended or aborted as the result of an unexpected Pay Connexion event, the remediation will be managed through our Client Service / Operations Practice Management team.			
T3.3.1	**Disaster Recovery Plan:** The Vendor should maintain a recovery test plan and recovery test procedures that result in a full recovery of the system following full and partial system failures.	Provide a copy of your recovery test plan and procedures, and provide documentation of periodic tests performed.	Expected
Please see *Attachment 5* for J.P. Morgan's Business Resiliency Summary.			

Data Management Requirements

Req#	Requirement Description	Required Response	Rating
T3.4.2	**Archived Data Access (Post Contract):** Authorized users must be able to receive a complete copy of current and archived data hosted by an ASP provider in the event of contract termination.	Explain how current and historical data can be received by the City if the contract is terminated for any reason.	Must Have
In the event that the City requires retrieval of historical transaction data after the contract term or termination, this information may be obtained after an authorized request is submitted to the same Pay Connexion Client Service team that will provide support during the contract term. Regardless, J.P. Morgan recommends independent archival of Pay Connexion remittance files and reports as the City requires.			
T3.4.1	**Off-line Storage:** Hosted solutions should support off-line storage of City data at City's site or elsewhere.	Describe how City personnel can create and periodically update off-line copies of City data. Explain the types of connections available to retrieve data and how data retrieval can be scheduled.	Expected

J.P. Morgan recommends that the City archive remittance files and reports independently as needed.

Authorized City personnel can access the administrative application, which is a robust customer service and payment reporting tool. All pages within the administrative application are compliant with section 508 of the Americans with Disabilities Act. The site is accessed through a secure URL. Each session is secured using Secure Sockets Layer (SSL) with 128-bit encryption technology.

Security measures are paramount and required to validate access to the reporting site. City "security officers" dictate access to the administrative site by defining administrative site functions to Client-defined role(s). The City then assigns individuals to each role. Individuals are also given secure user names and passwords to access the administrative application. Therefore, when an individual logs-in to the administrative site, they only see the functions necessary for them to perform their job.

Through Pay Connexion, the City will be provided with an online payment reporting tool to access your Daily Transaction Reports. Reporting capabilities are available through your administrative application, which allows you to view standard reports that include payment detail, payment summary, and credit card batch reports. Each report has different selection criteria that can be used to narrow the data of a selected report. The reports can be downloaded from the administrative application into Excel.

A daily remittance data file will be made available for download via the administrative site or through secure FTP.

This remittance file is the primary means to deliver remittance detail to the City. This standard format includes return data as well, and provides a daily means (Monday through Friday, excluding Federal Holidays) to reconcile funds settlement. The file is available in Extensible Markup Language (XML) and ASCII comma-delimited variable length formats. Authorized City administrators access the Pay Connexion administrative site from a standard web browser. The administrative site provides authorized City personnel with the ability to make payments, execute refunds (refund rules differ by payment method), generate a wide range of reports on demand, and perform other administrative functions.			
T1.4.2	**Data Storage Architecture**: The Vendor should explain how and where data is stored.	Describe the relationships between data stored on the main servers, the report servers, the training servers, the archive servers, and any off line data.	Expected
Please see our response to *Req # T1.1.5* above.			
T1.4.6	**Data Archiving:** The solution should provide a method for archiving historical data.	Explain the process for archiving historical data. Include information on archiving, retrieval, and purging record data and attached documents. Describe features available to authorized users for selecting records for archiving.	Expected
Transaction history is saved for 24 months (2 years) online, and an additional 5 years offline. By law, we are required to save this information for 7 years. Statement Images are retained online for 18 months. Archived information may be accessed by request to the Client Service / Operations Practice Management team.			
T1.4.8	**Field Level Validation:** The solution should perform forms-based data validation (field level validation) and display error messages when validation fails (i.e. user enters text in a numeric field).	Explain how the solution validates data entry and handles error messages and the level of criticality of each type of error (i.e. data validation, omitting a required field, etc.).	Expected
Pay Connexion performs forms-based data validation and displays error messages when validations fail (e.g., a payer enters an alpha character in a currency field). Validations occur not only on the Web and Admin channels but also with the transmission of inbound data via various interfaces such as the inbound files (e.g., Pre-Registration File, Statement Image Archive File), Web Services API methods, HTTPS Post and Web Services redirect session transfers. Response messages/codes/files are appropriate for the error type given the interface and enable the payer (if it is payer error) or administrative/IT personnel to troubleshoot.			
T1.4.9	**Transaction Log:** Tables or logs of transaction updates should be maintained that indicate the data element value(s) changed and the date, time, and User ID of the person making the change.	Describe how the solution uses tables or logs of transaction updates to indicate the data elements changed and the date, time, and User ID of the person making the change.	Expected
An audit trail is automatically generated as authorized admin users progress through the system and make modifications.			
T1.4.10	**Batch Load Data Validation:** If bulk or batch data loads are supported, the solution should use the same data validation criteria	If bulk or batch data entry is supported, explain the data validation performed by the application on the bulk loaded data.	Expected

	for bulk data loads as it does for manual data entry.		
Bulk/Batch data entry is supported via the Pre-Registration File and Statement Image Archive File. File and data validation is performed on these inbound files. Each file results in a response file which indicates the file success / failure and/or identifies specific issues with specific records to the City can refine its data and resubmit it.			
T1.4.13	**Backward Compatibility:** Future releases of the application should NOT render archived data unusable.	Describe how historically archived data is supported regardless of changes to the application data schema.	Expected
Future releases are backward compatible and do not render archived data unusable. At least the most recent three versions of each file and message type are supported.			
T1.4.14	**Transaction Validation:** The solution should include a transaction update confirmation or failure notification for user, batch and system administrator transactions. All such notifications to be logged and auditable.	Describe how the application informs the end user of success or failure of attempted transactions, including user transactions, batch transactions and system administrator transactions. Explain where notifications are logged, and how system admins can gain access to the logs.	Expected
Payers receive confirmation of successful transactions or appropriate failure messages in real time via the payment channel that is utilized for access. Payers may receive emails advising of batch activity (e.g., a prior ACH payment was returned, an instance of a recurring payment was processed, etc.) as well as activity executed by an admin user (e.g., a payment was refunded, a pending payment was cancelled, etc.).			

Interface Requirements

Req#	Requirement Description	Required Response	Rating
T3.10.1	**Data Mapping Definition:** The vendor must define data mapping, message formatting, required data elements for all data exchanges (both inbound and outbound) between City systems and Vendor-hosted systems	Provide details of the data interchanges between systems, including data types, formats, encryption, and requirements.	Must Have
Upon award, J.P. Morgan will provide a Functional Specification detailing feature descriptions as well as Connectivity and API Reference Guides detailing information and technical interfaces. This information will support the City's project scoping and development/integration efforts and will enable data mapping and message formatting for all in/outbound data elements. When the assigned Implementation Project Manager delivers the Build following the Configuration Requirements Definition phase of Implementation s/he will provide samples of all in/outbound interfaces (e.g., in/outbound files, Web Services API Methods calls and responses, HTML code, HTTPS Post messages, etc.) as applicable for the specific application configuration. Until the Configuration Requirements Definition phase of Implementation is completed, it remains unknown which interfaces and data elements will be in-scope for each application. If Web Services API methods are in-scope then an exchange of SSL certificates is required to support mutual authentication. If Real Time Payment Confirmation is in-scope then a supported SSL certificates is required to support encrypted			

HTTPS post messages.

If file transmissions are in-scope then appropriate measures are used for the selected Connectivity protocols (e.g., Secure FTP).

T1.5.5	**Data Interchange Definition:** The vendor should provide a detailed explanation of how any required data interchanges (real-time, near real-time or batch) are accomplished to and from other systems.	List and describe any/all real-time or near real-time data interchange to/from other systems required by the proposed solution. Include the data being transmitted, Protocol, Ports and level of encryption for each interface.	Expected

Please see our responses to *Req # T3.10.1* above as well as *Req # T1.6.4* below.

T1.6.4	**Standard Interface APIs:** The solution should use standard (published) API's for interfaces to other systems.	List the standard (published) API's that the solution uses to interface with other systems. List any proprietary APIs used.	Expected

Please see our response to *Req # T3.10.1* above.

FILES/MESSAGES SENT TO PAY CONNEXION FROM THE CLIENT:

Pre-Registration File (ASCII comma-delimited variable-length format)

This file is used by J.P. Morgan to 'register' payers into the Pay Connexion system prior to actual access through the IVR or the Web Application. The client generates this file every calendar day or every business day (depending on the application's configuration) with new payers, deleted payers or updates to existing, registered payers. This standard format provides a number of flexible options to the client. Record types include:

- User Profile Information
- Authorized Product Information
- Payment Information
- Payment Account Information (Requires PGP encryption)
- Product Parameters
- Recurring Payment
- Statement Information

Admin User Hierarchy File (ASCII comma-delimited variable-length format)

An as-needed transmission from the client to Pay Connexion that details the call-center reporting structure. This file assigns each admin user to a three-tier hierarchy, and is can be used by clients who wish to use the CSR Payment Reports.

Statement Image Archive File

This file allows the Client to load PDF formatted statements for their payer's to view in the Pay Connexion application. Statements are stored up to 18 months to allow payers to return to Pay Connexion and review past statements. Clients electing to use this file must also use the Pre-Registration file.

Web Channel Session Transfer

In order to access the J.P. Morgan Pay Connexion Web Channel, the client must pass the appropriate parameters to their configured Pay Connexion application through either an HTTP Post or Web Service API. These parameters are defined during the implementation process. Web Service APIs are required for various functions, as detailed later in this document.

Administrative Channel Session Transfer

In order to access the J.P. Morgan Pay Connexion Administrative Channel, the client can either have their administrative users access the Pay Connexion Administrative Channel through a URL entered in their Internet browser, or can pass the appropriate parameters to their configured Pay Connexion application through a Web Service API. These parameters are defined during the implementation process.

FILES AND MESSAGES SENT/AVAILABLE TO THE CLIENT FROM PAY CONNEXION:

Remittance File

This file is used as the primary means to deliver remittance detail to the client. This standard format includes return data as well, providing clients with a daily means (excluding Federal Holidays) to reconcile funds settlement.

Pre-Registration Response File

This file is used by J.P. Morgan to convey back to the client the results of the load process for the pre-registration file received every business day.

Payment account change File

A daily transmission (Monday through Friday, excluding Federal Holidays) that provides you with information regarding payment accounts changed in Pay Connexion by Payers, administrative users, or NOC's.

Recurring Payments File

A daily transmission (seven days a week, including weekends and Federal Holidays) that provides recurring payment activity from the previous day. All new, edited, stopped, and expired recurring payments are included in the file.

Fraud Detection Report

The Fraud Detection report is provided to help the Client detect suspicious Payer activity. The report is downloaded from the administrative channel, as needed.

Statement Image Response File

This file is used by J.P. Morgan to convey back to the client the results of the load process for the Statement Image Archive file.

User Activity File

This file is used by J.P. Morgan to convey back to the client the results of payer's changes to their Pay Connexion settings.

Real Time Payment Confirmation

This message contains payment activity performed by a payer or administrator either over the Web or through the IVR. This message is sent over the Internet via https, and is sent every day, including weekends and holidays, immediately upon completion of a payment action. A full listing of the record types sent is described later in this document.

All Times are Eastern.

For items stated in the chart below that reference Federal Business Days, please refer to the Federal Reserve Holiday schedule at http://www.federalreserve.gov/releases/k8/default.htm for days that are not considered "Federal Business Days".

Table 11 - Files and Messages

Name	Purpose	Format	Delivery Method

Remittance File	File of Pay Connexion remittance data provided to the client to reconcile funds settlement	XML CSV	Download from the Admin Channel File transfer via J.P. Morgan Connectivity Services
Pre-Registration File	Used by clients to 'register' payers into Pay Connexion prior to accessing the IVR or Web	CSV	File transfer via J.P. Morgan Connectivity Services
Pre-Registration Response File	Conveys to the client the results of the load of the pre-registration file	CSV	File transfer via J.P. Morgan Connectivity Services
Payment account change File	Conveys to the client any changes made within Pay Connexion to payer's payment account information	CSV	File transfer via J.P. Morgan Connectivity Services
Recurring Payments File	Conveys to the client any recurring payment set-up activity (Starts, Edits, Stops)	CSV XML	File transfer via J.P. Morgan Connectivity Services
Admin User Hierarchy File	Optional client file to convey details of their call center reporting structure.	CSV	File transfer via J.P. Morgan Connectivity Services
Fraud Detection Report	Conveys to the client possible suspicious Payer activity	CSV	Downloaded from the Admin Channel
Statement Image Archive File	Used by clients to load statement images for viewing on the Web	zip tar tar.gz	File transfer via J.P. Morgan Connectivity Services
Statement Image Response File	Conveys to the client the results of the load of the Statement Image Archive File	CSV	File transfer via J.P. Morgan Connectivity Services
User Activity File	Conveys to the client changes to Payer Settings	CSV	File transfer via J.P. Morgan Connectivity Services

Table 12 -Real-Time Communication Summary

Name	Purpose	Format	Connectivity	Notes
Real Time Payment Confirmation	Provide near real-time updates to the client's back-end	XML URL	HTTPS	DTD provided Client must open

(RTPC)	system(s) each time a payment is initiated, edited, canceled, or refunded	Encoded		firewall and port and allow a POST Client must respond with a single line HTTPs OK
Web Session Transfer – HTTP Post	Used to connect client's site to Pay Connexion	HTTP	HTTP	HTML provided during implementation HTTP Method is a "POST"
Web Session Transfer – Web Services	Used to connect client's site to Pay Connexion in order to pass in sensitive information	Web Services API	Web Services API	Web Services required. Please refer to the API Reference Guide.

Web Services API Methods Including:

Initiate Public Session Transfer

The Initiate Public Session transfer web service allows a biller to send all public session transfer information as part of this web service to PCX. System will validate all the fields that are passed in as part of web service. If there are any field level format validation error or if the data is not as per the business rules, system responds with a return reason code. If all the information is valid, system saves the information in an internal table in PCX and will generate a unique session transfer ID to be saved as part of that table. As part of the success response, system will send a URL that has the PCX web name, biller id, biller group id and session transfer id.

Initiate Admin Session Transfer

The Initiate Admin Session transfer web service allows a biller to send all Admin session transfer information to PCX as part of this web service. System will validate all the fields that are passed in this web service. If there are any field level format validation errors or if the data is not as per the business rules, system responds with a return reason code. If all the information is valid, system saves the information in PCX and will generate a unique return session transfer ID to be saved as part of that information. As part of the success response, system will send a URL that has the PCX web site link, biller group id, biller id and session transfer id

Register/Update User Profile

This method allows a client to create and update payers in Pay Connexion. If the combination of the biller group ID, biller ID, and user Id already exists the system will attempt to update the already created user. Therefore, every new user Id must be unique to create a new user in Pay Connexion. Creating a user is required as part of all web service and hosted functionality except unregistered payments.

Register/Update Payment Account

This method allows a client to add and update payment accounts in Pay Connexion for their registered payers. The client will be required to supply a biller group ID, a biller ID, user Id, and a set of account information. The system will attempt, using the unique fields that are part of an account, to search for an already existing account. If an account exists, the system updates that account. Otherwise, the system will insert a new account for that payer.

Get Payment Accounts

This method allows clients to retrieve one to many accounts given a supplied user ID. The accounts being

returned will be of the Account complex type and include the Account ID of each.

Delete Payment Account

This method allows clients to remove a previously created Payment Account from the Pay Connexion system. This can be accomplished be either sending Pay Connexion an Account ID or a full set of payment account information. Only payment accounts with no pending or active recurring payments can be removed.

Make Single Registered Payment

This allows clients to make or edit a payment in Pay Connexion. In the case of card payments, if the payment is not successful (declined, CVD error, etc...) Pay Connexion will only return the authorization information. In other cases, for a successful payment the client will receive the payment object.

Make Single Unregistered Credit Card Payment

This method will allow clients to make credit card payments for payers not registered in PCX. If the payment is not successful (declined, CVD error, etc...) Pay Connexion will only return the authorization information. In other cases, for a successful payment the client will receive the payment object.

Make Single Unregistered ACH Payment

This method allows a client to make ACH payments for payers not registered in PCX. For a successful payment the client will receive the payment object.

Make Single Unregistered ATM Payment

This method allows a client to make ATM payments for payers not registered in PCX. For a successful payment the client will receive the payment object.

Get Single Payment

This method allows clients to retrieve a historical or pending main payment using the transaction confirmation ID Pay Connexion generated or the Payment Reference ID supplied by the client.

Cancel Single Payment

This method allows a client to cancel a pending, non-recurring instance, main payment, by sending Pay Connexion the transaction confirmation ID of the pending payment. If a payment was successfully cancelled, Pay Connexion will return the payment object in the cancelled state.

Get Convenience Fee

This method allows clients to calculate what the convenience fee will be for a payment before a payment is made. Pay Connexion can charge different fees depending on a number of factors. The request message requires several elements in order to calculate the fee. The response returns a single fee.

Void Payment

This method allows a client to void a payment, by sending Pay Connexion the transaction confirmation ID of the payment. If a payment was successfully voided, Pay Connexion will return the payment object.

Please note: This method specific to the Paymentech Global platform.

Refund Payment

This method allows a client to refund a payment, by sending Pay Connexion the transaction confirmation ID of the payment. If a payment was successfully refunded, Pay Connexion will return the payment object in the refunded state. This method allows refunds on ACH, Credit Cards and ATM payments.

Add/Update Statement Info

The Update Statements Info web service adds / updates statements for a specific user. If a statement

already exists for the payor, system will update the statement. If a statement does not exist, system will add that statement to the user.

Update User Profile and Make Single Payment

This method allows a client to create or update payors In Pay Connexion. This method also creates or updates a payment on behalf of an existing registered payor.

If the combination of Biller group ID, Biller ID and user ID already exists, the system will attempt to update the already created payor. Therefore every new user ID must be unique to create a payor in Pay Connexion. Similarly on the payment front, when a payment confirmation number value is passed in, system will attempt to edit that payment. If no payment confirmation number is passed in, a new payment is created. This API requires the biller to pass in both user profile and payment information as part of the API response.

Pay Connexion's Web Services API Methods use industry standards and best practices. These include:

- W3C – SOAP 1.2 - SOAP Lightweight protocol intended for exchanging structured information in a decentralized, distributed environment. This messaging framework uses XML technologies, an extensible messaging framework containing a message construct that can be exchanged over a variety of underlying protocols.
- WS-I Basic Profile 2.0 - This is a set of non-proprietary web services specifications, along with clarifications, refinements, interpretations, and amplifications of those specifications, which promote interoperability.

Every Biller that uses Pay Connexion's API will be required to follow the mutual authentication scheme. This involves the City installing a certificate on their server and J.P. Morgan installing a certificate on its Pay Connexion server. All messages will also be required to be sent over HTTPS. Therefore, you can be confident in the following:

- You, as the Biller, can be sure you're communicating with Pay Connexion
- Your communication with Pay Connexion is encrypted, so others can not intercept it
- You have verification that the message received relates to the message sent

Additional technical information is provided during Pay Connexion's implementation process.

T1.6.8	**APIs to Support RPC via Web Services:** The solution's API may support remote procedure calls via web services.	Provide information on the use of web services available in the API for interfacing with other systems.	Desired

Please see our response to *Req # T1.6.4* above.

T1.6.1	**SMTP/Microsoft Exchange Compliant Email:** If email is used within the application, the email component may be SMTP and/or Microsoft Exchange compliant and provide a messaging development environment through the provision of documented APIs.	Describe the application's messaging architecture, and indicate if the solution is SMTP and/or Microsoft Exchange compliant and how it provides a development environment through the provision of APIs.	Desired

Depending on the application configuration Pay Connexion generates several outbound email messages that are delivered to users who provide an email address. Emails sent by Pay Connexion will be sent in an HTML format as well as the standard text format. The type of email displayed is dependent on the email application used. Emails returned for various reasons (incorrect email address, SPAM filter, etc.) are dropped and are not provided to the biller for follow-up. Payments initiated over the IVR do not generate confirmation emails.

Billers will have the option to include images in HTML emails. An image may be displayed at the top of each email as well as the bottom. Email images are set at either the Biller or Biller Group level. The total email file size with graphics should not exceed 100k. GIF is the recommended image format, but JPG is acceptable. The total

header content should not exceed 500 width x 100 height in pixels. The total footer content should not exceed 500 width x 50 height in pixels.

Emails may be delivered for the following payment and registration activities:

Statement Notification

- ✓ New Statement is available for viewing in the application

Single Payment

- ✓ E-check payment is initiated on the web and admin site only
- ✓ Debit/Credit Card payment is initiated on the web and admin site only
- ✓ ATM Card payment is initiated on the web and admin site only
- ✓ E-check payment is edited on the web and admin site only
- ✓ Debit/Credit Card payment is edited on the web and admin site only
- ✓ ATM Card payment is edited on the web and admin site only
- ✓ E-check payment is processed
- ✓ E-check payment is returned
- ✓ Warehoused E-check payment is cancelled
- ✓ Warehoused card payment is processed
- ✓ Warehoused credit/debit card payment is declined
- ✓ Warehoused ATM card payment is processed
- ✓ Warehoused ATM card payment is declined

Recurring Payment

- ✓ Recurring payment is initiated
- ✓ Recurring payment is edited
- ✓ Recurring payment is stopped
- ✓ Recurring payment is about to end

Recurring Payment Instance

- ✓ Recurring E-check payment instance has been processed
- ✓ Recurring credit card payment instance has been processed
- ✓ Variable recurring payment – payment information update
- ✓ Variable recurring payment – due date occurs after the expiration date
- ✓ Variable recurring payment – amount due is greater than maximum payment amount

Registration

- ✓ Registration Confirmation

Password

- ✓ Forgot Password
- ✓ Reset Password

Credit Cards

- ✓ Credit Card Expiration Warning

Refunds

- ✓ E-check payment is refunded
- ✓ Credit card payment is refunded

Cancellations

- ✓ E-check payment is cancelled
- ✓ Credit card payment is cancelled
- ✓ ATM payment is cancelled

Payer Account

- ✓ Payer account updated
- ✓ Payer account removed

Reports

- ✓ Report request has been processed
- ✓ Report returned too many records

Spanish e-mails are available through recurring transactions, warehoused transactions or those initiated by the public and administrative sites. The following is a list of the Spanish e-mails available from Pay Connexion.

Single Payment

- ✓ E-check or card payment is initiated on the web and admin site only
- ✓ E-check or card payment is edited on the web and admin site only
- ✓ E-check payment is processed
- ✓ E-check payment is returned
- ✓ Warehoused E-check payment is cancelled
- ✓ Warehoused card payment is processed
- ✓ Warehoused card payment is declined

Recurring Payment

- ✓ Recurring payment is initiated
- ✓ Recurring payment is edited
- ✓ Recurring payment is stopped
- ✓ Recurring payment is about to end

Recurring Payment Instance

- ✓ E-check or card recurring payment instance is processed
- ✓ Variable recurring payment – payment information update
- ✓ Variable recurring payment – due date occurs after the expiration date
- ✓ Variable recurring payment – amount due is greater than maximum payment amount

Registration ✓ Registration Confirmation **Password** ✓ Forgot Password **Credit Cards** ✓ Credit Card Expiration Warning **Refunds** ✓ E-check or card payment is refunded **Cancellations** ✓ E-check or card payment is cancelled			
T1.6.2	**Supported Data Formats:** The solution may support the import/export of data from/to various other data sources/repositories.	List the various data sources and data formats that the system imports/exports. (i.e. comma delimited, text, HTML, XML, SQL, etc.).	Desired
Please see our response to *Req # T1.6.4* above.			
T1.6.3	**Supported Report Formats:** The solution may generate reports in a variety of file formats, including XML, PDF etc.	Describe the solution's process for generating reports and data extracts files in a PDF format. List all formats allowed by your application.	Desired
T1.6.7	**Reports Compatibility:** Reports provided by the application may be compatible with Crystal Reports and other reporting providers.	Describe how the system's reporting is compatible with Crystal Reports and other reporting vendors (e.g. Cognos, MicroStrategy, QuickView)	Desired

Please see our response to *Req # T1.6.4* above.

Pay Connexion reports provide very flexible filtering capabilities by allowing your users to select parameters for downloading data. For example, reports can be run with specific date ranges, dollar ranges, product types (as applicable), payment types (card, ACH, etc.) and payment channels (web, IVR, admin). By combining these various parameters, the client has the ability to narrowly define the specific data your wish to download. Reports can also be sorted by each of the columns displayed in the report results. The reports are either produced in batch or real time, and can be viewed online, printed, and downloaded to the desktop of the administrative user. The following types of reports are available through the administrative site:

- Payment Detail Report (HTML – View Online / Download as CSV)
- Product Detail report (HTML – View Online / Download as CSV)
- Payment Summary Report (HTML – View Online / Download as CSV)
- Recurring Payment Report (HTML – View Online / Download as CSV)
- Product Recurring Payment Report (HTML – View Online / Download as CSV)
- Card Batch Report (HTML – View Online / Download as CSV)
- Fraud Detection Report (Download as CSV)
- Administrative User Access Report (HTML – View Online / Download as CSV)

- Download Remittance File (Download or receive via Connectivity as CSV or XML)
- CSR Payment Report (Summary/Detail – Daily/Weekly/Monthly (PDF – View Online / Download as CSV)

Network Requirements

Req#	Requirement Description	Required Response	Rating
T1.7.4	**Verifiable Time Source:** The system must use an accurate, verifiable time source. The solution may use the server time which is already utilizing NTP.	Explain how the solution applies a traceable time stamp such as GPS clock, NTP or Stratum time source for a traceable time stamp for transactions or key events.	Must Have
Pay Connexion utilizes an accurate, verifiable time source for time stamping transactions and other traceable key events.			
T1.7.5	**Synchronized Time/Date Stamp:** The system should synchronize time/date stamp between client-side components and back-end servers.	Indicate whether the application client components are synchronized with the back-end components, and explain how the synchronization occurs.	Expected
Pay Connexion utilizes an accurate, verifiable time source for time stamping transactions and other traceable key events.			
T1.7.3	**DNS Component Identification:** The Vendor should use standard Domain Name Services (DNS) for identifying all server components in the system.	Explain how that the system uses standard Domain Name Services (DNS) for identifying all server components in the system.	Expected
J.P. Morgan adheres to leading practices with respect to identifying server components in the system.			
T1.7.7	**Standard MIB Files (SNMP):** If the proposed system components support SNMP, the Vendor should provide standard MIB files for all SNMP-enabled components.	Provide a list of SNMP MIBs available and supported by the proposed system.	Expected
Please see our response to *Req # T1.6.4* above.			

Performance Requirements

Req#	Requirement Description	Required Response	Rating
T1.8.2	**Concurrent Users**: The system should be capable of supporting a number of concurrent users within documented parameters without any system modification to the application as proposed.	Describe the application limitations for concurrent use. Describe system requirements for growth beyond the specified number of concurrent users.	Expected
The proven Pay Connexion platform is being used today by other clients to process over 19 million annual transactions totaling over $64 billion. The Pay Connexion IT department regularly performs system capacity planning and analysis of future growth. Currently, the Pay Connexion environment is adequately architected (server size, disk space, etc.) to handle the current volumes as well as projected growth. Additional Storage Area Network (SAN) is forecasted and SAN allocation is monitored regularly to ensure we have adequate space to accommodate future growth. As we add volume, we expect the system to continue to scale. As a general rule,			

we move to increase capacity once we transaction volume reaches 60% of available capacity.			
T1.8.1	**Transparent Backup Process:** The system should provide a backup process that does not impact the performance of the core system or the availability of online data.	Explain how backup processes do not impact core system performance or availability of online data. If the proposed solution does not include a backup tool, recommend one that has been tested with your system.	Expected

J.P. Morgan will provide a redundant transaction processing system to backup the primary transaction processing system. Both will be supported by necessary contingency planning to ensure that disaster recovery processes will support transaction processing in the event of a disruption affecting the primary system. In the event of a failure of the primary transaction processing system, the backup system will be deployed within one hour of the primary system outage.

J.P. Morgan operates its highly available, fully-hosted Pay Connexion solution at two geographically dispersed data centers, a primary and a "hot" backup. The equipment located at the backup data center mirrors that at the primary data center in sizing and configuration. At each tier, (i.e., Web, Application and Database), the components of Pay Connexion are configured identically at each data center. In the event of an emergency or disaster, recovery operations simply involve switching the networking components from the primary data center to the backup data center. Normal business operations can then resume at the backup data center within the stated service level agreements.

Each J.P. Morgan business unit performs a formal business impact analysis to assess the operational, financial and reputation impact of a service disruption on clients and the firm. The results of the business impact analysis are used to determine the criticality of the function and the corresponding recovery time objective.

Recovery time objectives and service levels vary based on criticality of the specific business function. For our most critical functions, we apply a two-hour recovery time objective for full resumption of normal operations. For the least critical functions, we apply a recovery time objective of 73 hours, which results in those business functions deferred and/or suspended.

Business and support group areas must identify their requirements based on their process capacity needs to address a loss of an entire zone for a minimum of 30 days. This enables businesses and support groups to stage their recoverability over that time period.

We conduct a live cutover to our backup processing site for a full 24 hours. This process helps to validate that all components are tested each year providing a high level of confidence that we can move to our backup site, if needed. All test results and business continuity plans are reviewed by our internal auditors and as part of an annual independent operational audit.

The diagram below illustrates Pay Connexion's operating environment.

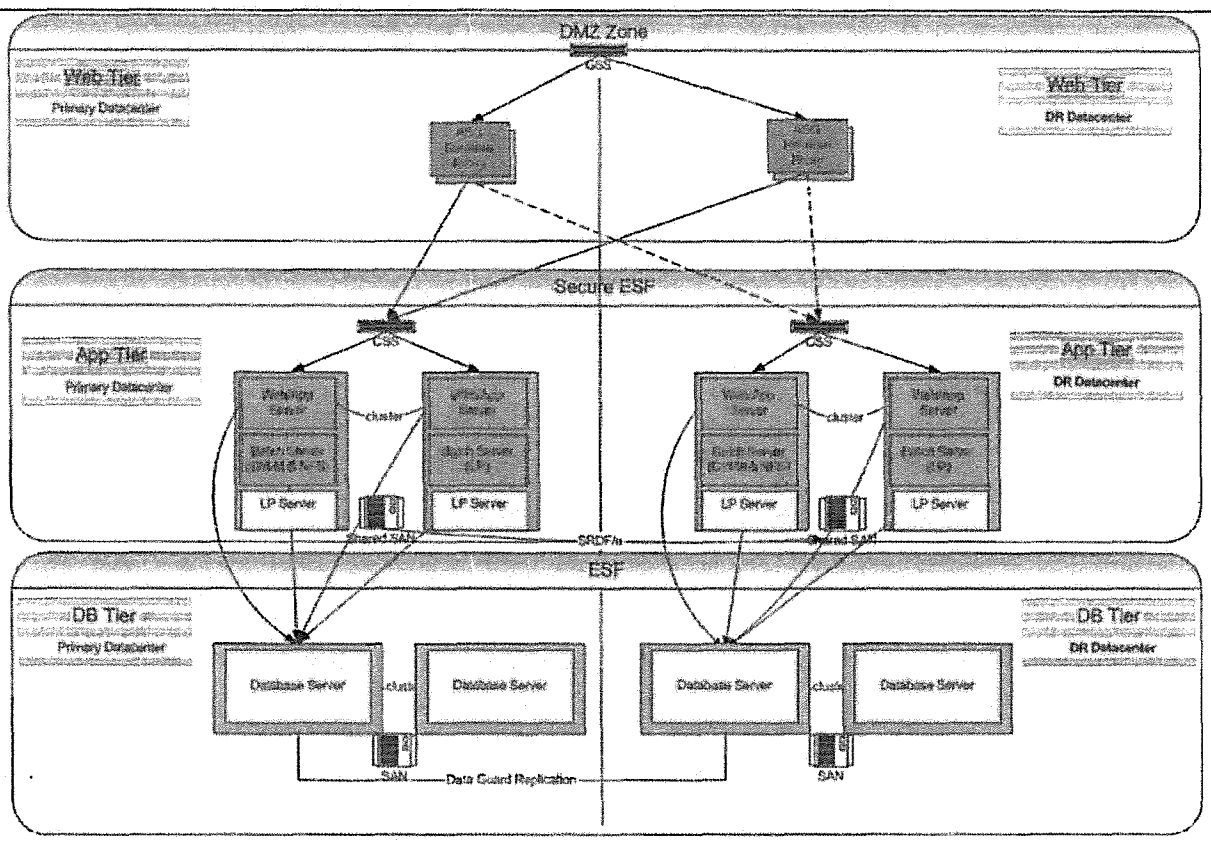


Figure 14 Primary and Disaster Recovery Operating Environment

Pay Connexion's operating environment offers several disaster recovery protections:

- Data Centers
  - Two Geographically Dispersed Data Centers: Primary and DR
  - Virtual Servers shared with Pay Connexion
  - Shared IVR infrastructure with Pay Connexion
  - Shared DR/UAT environment
- Hardware Architecture
  - SSL offload
  - Dual active web server
  - Dual active application server
  - Clustered active/standby database server
  - DR database servers replicated

T3.12.1	**Transaction Speed:** The system should be capable of processing transactions within documented parameters.	Provide data that explains the average transaction time per 1,000 transactions, including best and worst metrics.	Expected

The Pay Connexion IT department regularly performs system capacity planning and analysis of future growth. Currently, the Pay Connexion environment is adequately architected (server size, disk space, etc.) to handle the current volumes as well as projected growth. Additional Storage Area Network (SAN) is forecasted and SAN allocation is monitored regularly to ensure we have adequate space to accommodate future growth. As we add

volume, we expect the system to continue to scale. As a general rule, we move to increase capacity once we transaction volume reaches 60% of available capacity.

Table 13 - System Capacity

Approximate Throughput per	Transactions	Dollars
Year	19,000,000	$64,000,000,000
Month (12)	1,583,333	$5,333,333,333
Day (30)	52,778	$177,777,777
Hour (24)	2,199	$7,407,407
Minute (60)	37	$123,457
Second (60)	0.6	$2,058

Card transactions are authorized (or declined) within three seconds.

T3.13.2	**Meeting Service Performance Targets:** The proposed system should be capable of meeting service performance targets by modifying, adding capacity, increasing bandwidth, etc.	Explain the proposed system components that will be used to meet the requirement.	Expected

Please see our response to *Req # T3.12.1* above.

T3.14.1	**24x7 Support:** The vendor should provide 24x7 support availability to the city.	Describe how the system is supported by the vendor including availability and support channels (e.g. telephone, email, online chat)	Expected

J.P Morgan's Pay Connexion Production Management Practice team will provide the City with customer support, including assistance answering technical and transactional questions. Our support team will provide an immediate answer or open a reference ticket to research the specific question and return your call. Our Production Support hotline is available 24 hours a day, every day via a toll free telephone number and email.

Should escalation be required, our e-Payment Solutions team is available. This team is experienced and empowered to commit the resources of the firm. Behind them stand many cross functional specialists who have extensive experience with the various aspects of these types of solutions.

In addition, your relationship manager and your Treasury Sales Management Officer are ultimately responsible for your satisfaction with all of J.P. Morgan services and are always available to assist you with anything you may need.

Security Requirements

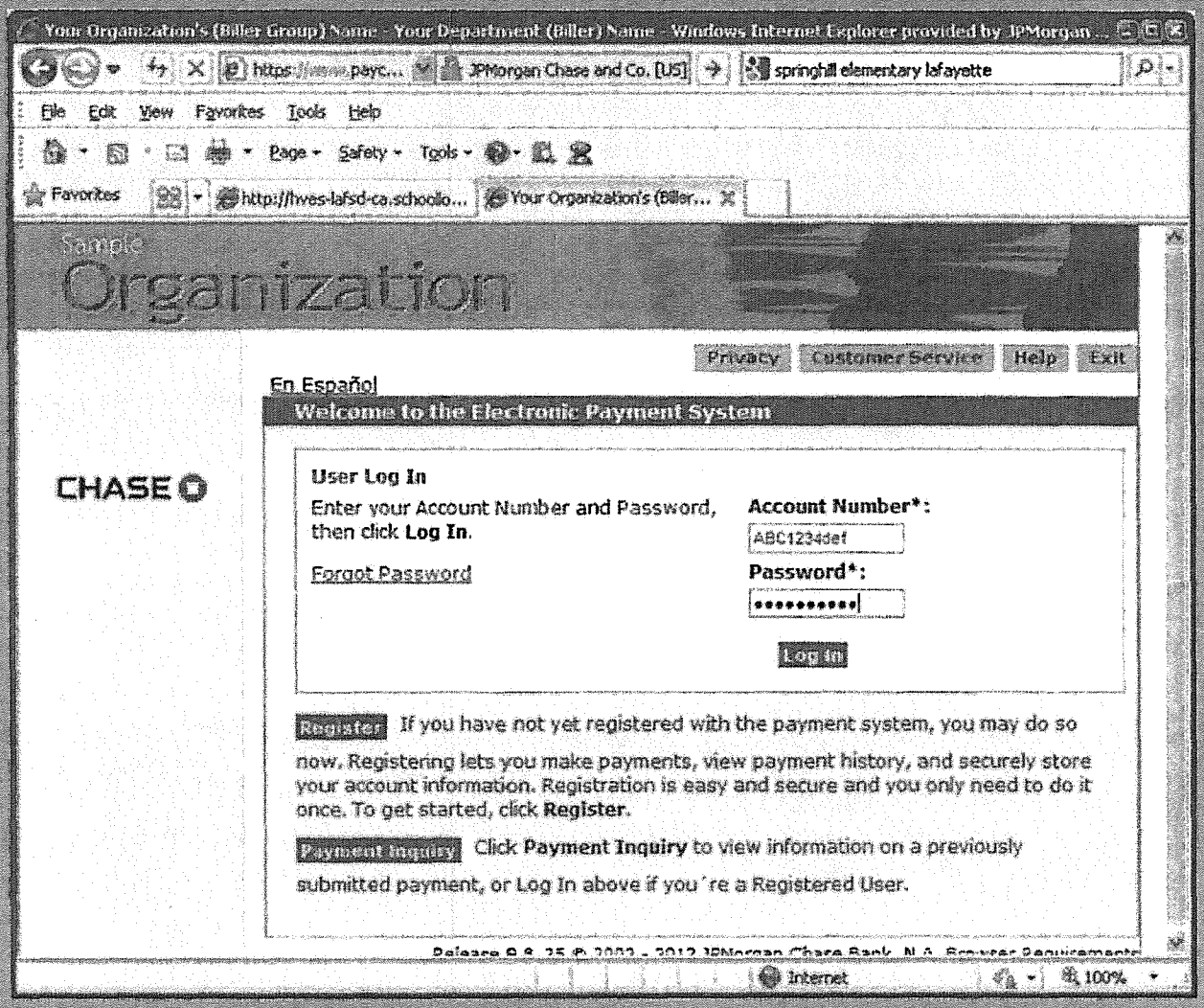
Req#	Requirement Description	Required Response	Rating
T1.9.12	**Secure Session Communication:** If the solution provides a Web server, the solution's Web interface must be able to operate a secure communication session as SSL 128 bit encrypted HTTPS.	Describe how the solution's Web interface is able to operate a secure communication session as SSL 128 bit HTTPS.	Must Have

Each session is secured using Secure Sockets Layer (SSL) with 128-bit encryption technology. Session transfers

into the Web channel may be HTTPS Post or be executed via supported by a redirect per the Web Services API Method Initiate Public Session Transfer (Please see our response to Req # T1.6.4 above.).			
T1.9.1 5	**Minimum Password Storage and Transmission Standards:** Passwords must not be stored unencrypted in cache, or transmitted as clear text over the network.	Explain how passwords are managed, stored and transmitted over the network.	Must Have
Please see our response to *Req # F501 and Req # F518.* Pay Connexion's turnkey application is a high performance, adaptable solution that can fully accommodate the City's current and future payment volume. We are confident that our solution will integrate effectively with the City's existing system and will allow the City to process payments, report on remittances, and manage payer information quickly and accurately. In addition, our solution is extremely secure, using leading security measures when protecting users' credit card data. User information is both encrypted and transmitted over encrypted channels, regardless of the selected transportation method. Passwords are stored in a one-way hash. Sensitive credit card information, such as credit card number and expiration date, is encrypted using the triple data encryption standard (DES) algorithm. In addition, our policies ensure that data is protected against unauthorized user access. J.P. Morgan recognizes the paramount importance of the confidentiality, integrity, and availability of personal and e-payment related data. Pay Connexion e-payment solution utilizes industry leading security measures and is certified as being Payment Card Industry (PCI) compliant. The PCI-DSS certification confirms that we have taken the appropriate measures to ensure that we are protecting the City, the payer, and the card processing system from credit card fraud and other risks. These steps include requirements for security management, payment policies, data storage procedures, network architecture, software design, and other payment system measures.			
T3.9.1	**Annual Security Audits:** The vendor must conduct a 3rd party annual security assessment of all tiers of its hosting facility, including application servers and network devices. Copies of the security audit reports shall be provided to the City annually.	Describe how an external audit of the proposed system security will be provided. Specify what type of security audit is performed.	Must Have
For Pay Connexion a full PCI-DSS audit is completed annually, and network scans are performed on a quarterly basis. Audits are completed by a qualified and certified independent third party audit firm, which in the case of Pay Connexion is Jefferson Wells. Pay Connexion is listed with PCI-DSS as compliant (Level I), receiving a favorable rating from the assessor during the March 31, 2012 audit. Included in the PCI-DSS review is establishing and maintaining a secure network, protection of card holder information, data access and controls, and regular system and network monitoring. Proof of PCI-DSS Compliance can be found at: Visa: http://usa.visa.com/download/merchants/cisp-list-of-pcidss-compliant-service-providers.pdf Search on "Pay Connexion" MasterCard: http://www.mastercard.com/us/company/en/docs/SP_Post_List_2012.pdf Search on "PayConnexion"			
T3.9.6	**PCI Compliance:** The vendor must be PCI-compliant (Level 1) and shall remain compliant through the life of the contract.	Provide evidence of PCI compliance. Provide PCI audit results from previous audits.	Must Have
Please see our response *to Req # T3.9.1.*			
T3.9.8	**Distribution of City Data:** City data must not be made available to any other parties	Describe how City data is protected from	Must

	not specifically authorized to view or access the data.	access by unauthorized parties.	Have
Our solution is extremely secure, using leading security measures when protecting users' credit card data. User information is both encrypted and transmitted over encrypted channels, regardless of the selected transportation method. Passwords are stored in a one-way hash. Sensitive credit card information, such as credit card number and expiration date, is encrypted using the triple data encryption standard (DES) algorithm. In addition, our policies ensure that data is protected against unauthorized user access. J.P. Morgan recognizes the paramount importance of the confidentiality, integrity, and availability of personal and e-payment related data. Pay Connexion e-payment solution utilizes industry leading security measures and is certified as being Payment Card Industry (PCI) compliant. The PCI-DSS certification confirms that we have taken the appropriate measures to ensure that we are protecting the City, the payer, and the card processing system from credit card fraud and other risks. These steps include requirements for security management, payment policies, data storage procedures, network architecture, software design, and other payment system measures.			
T1.9.13	**Minimum Password Standards:** The solution should provide and enforce complex password formats. Passwords shall be a minimum of 8 characters, and shall allow use of upper and lower case and numeric and special characters.	Explain all password format options provided by the solution, and how passwords are managed and enforced.	Expected
Payer passwords may exceed 8 upper/lower case alphanumeric or numeric characters and special and control characters are allowed. Please note that the format for passwords (and user IDs) for applications that support payments by pre-registered IVR payers must be all-numeric due to the usability constraints of a telephone keypad as the user interface.			
T1.9.14	**Non-displaying Passwords:** Passwords should not be displayed as readable text when users are entering them on-screen.	Describe how system allows end users to type in their password in a non-printing, non-displaying manner (i.e. ****).	Expected

Passwords are not displayed as readable text when entered on the screen. See below screen shot:



T1.9.1 6	**Support for Tiered User Permissions:** The solution should be capable of supporting tiered user permissions to provide application security.	Explain/Describe the tiered permission capabilities the solution offers. Explain how roles/groups/permissions are defined and assigned.	Expected
Please see our response to *Req # F501* above.			
T1.9.3 2	**Multiple Security Roles:** The solution should allow for multiple security roles for users (i.e. Admin, Supervisor, Staff etc.) with appropriate permissions.	Describe how the solution functions in relation to user roles including any predefined roles and their system access. Discuss both application software and DB management user permissions.	Expected
Please see our response to *Req # F501* above			

T1.9.3 3	**Changing Passwords:** If the solution provides the means of user authentication, it should provide the ability for system users to change their active or expired passwords.	Describe how end users can change their passwords, both current and expired.	Expected
Please see our responses to *Req # F518 and Req # F507* above			
T3.9.2	**Time Stamped Access Logs:** All user access should be logged with time-stamped entries, and the log made available to the City.	Describe what user access logs are kept and made available to the City, and how they are accessed.	Expected
An audit trail is automatically generated as authorized admin users progress through the system and make modifications.			
T.11.3	**SAS 70 Audit Compliance:** The system should meet SAS 70 requirements.	Describe how the system is SAS 70 audit compliant.	Expected
JPMorgan Chase Bank, N.A. has not engaged a public accounting firm to perform a Statement on Standards for Attestation Engagements No. 16, (SSAE 16), formerly referred to as a SAS 70, examination of our Treasury Services operations and therefore we cannot offer a SOC 1 certification report. However, J.P. Morgan does have an effective internal risk framework designed to provide a sound and well-controlled operating environment. This includes rigorous Operational Risk Management and Information Technology Risk Management programs, which are designed to meet or exceed the requirements of the Office of the Comptroller of the Currency (OCC) and Federal Financial Institution Examination Council (FFIEC). The programs include assessment and testing of operating and technology controls, complemented by policies, procedures and key risk metrics and a comprehensive, risk-based internal audit program. Should the City have more specific questions about the details of J.P. Morgan's internal controls, they may be formally answered upon request.			
T1.9.1	**Remote Application Update Permissions:** The solution should not require operating system administrator privileges on the client workstation(s) to run or receive application updates.	Describe the level of privileges required to install application updates and indicate if the application requires workstation administrator privileges to execute or update.	Expected
Pay Connexion admin user access is entirely browser-based. New Pay Connexion functionality is deployed via periodic product releases. There are typically three to five product feature releases annually, each of which includes functionality which is developed internally and tested extensively. Minor/Maintenance releases may also be deployed throughout the year. Planned outages are taken as needed for purposes such as the release of new functionality and other maintenance. In the event of a planned outage, notice is given at least 24 hours in advance of the scheduled outage. Downtime is scheduled within a standard window of Sunday 1:00 a.m. to 7:00 a.m. ET.			
T1.9.2	**Bulk Data Secure Network Transport:** If bulk data loads via the Internet are supported by the solution, a secure network transport method for bulk data should be supported.	Describe how the solution supports secured and/or encrypted transports of data if bulk data load is supported via the Internet.	Expected
All in-scope files may be transmitted by secure means of Connectivity such as Secure FTP.			
T1.9.3	**Security Permissions Default:** When new users are created, the security permissions assigned to the new accounts should default to least privileged.	Describe the process of creating a new user in the system, and explain the default system privileges assigned to new user accounts.	Expected

Please see our response to *Req # F501* above.			
T1.9.4	**Activity Monitoring:** The system should enable authorized users the ability to monitor (in near real-time) and report on data access activities for a particular user, group, application, device, and file.	Describe how the solution provides real-time capability to selectively monitor and report on data access activities for a particular user, group, application, device, and file.	Expected
Please see our response to *Req # F501 and Req # T1.6.3* above. Among the real time reports and data available to the City's authorized admin users through Pay Connexion's administrative site are payment and product summary and detail reports, payor profile, statement and history data, admin user access privileges and more. The admin site provides administrators with great deal of visibility into system activity.			
T1.9.5	**External Transaction Tracking:** The solution should provide authorized users the ability to track and log all transactions originating from external network sources.	Describe how authorized users track and log all transactions originating from external network sources. Verify that log data includes destination host IP address, originating source host IP address, date, and time.	Expected
Pay Connexion provides authorized admin users with indication of the Pay Connexion payment channel that a payer accessed in making each payment.			
T1.9.9	**IP Port/Protocol Minimization:** The solution should minimize the number of different IP ports and protocols to limit exposure and simplify security administration.	Describe how the solution minimizes the number of IP ports and protocols used and provide a list of IP ports and protocols utilized.	Expected
Upon award, specific detail will be provided regarding the IP range to which the City's firewall must be opened and additional information will be provided regarding protocol to limit exposure and simplify security administration.			
T1.9.17	**Encrypted Data Transport:** The solution should provide a secure method of data transport that encrypts application data sent between the front-end user system and the back-end servers.	Describe the encryption methodologies provided by the solution for transport of application data.	Expected
With our Pay Connexion System, access to mainframe based information systems residing behind a firewall occurs through batch files securely transferred through the Internet. Pay Connexion uses leading security measures when protecting users' credit card data. User information is both encrypted and transmitted over encrypted channels, regardless of the selected transportation method. Passwords are stored in a one-way hash. Sensitive credit card information, such as credit card number and expiration date, is encrypted using the triple data encryption standard (DES) algorithm. Each session is secured using Secure Sockets Layer (SSL) with 128-bit encryption technology. Strict access control and physical security safeguards are implemented at both the primary and backup data centers to maintain a controlled, limited access environment for the areas supporting our payment solutions. Payment account data is encrypted in storage and is always masked when displayed within our payments solution, with only the last 4 digits available for identification (e.g., XXXXXXXXXXXX1234). To prevent unauthorized user access, we employ security measures to either the system or the data (compliance			

with PCI-DSS, CISP, SDP, etc.). J.P. Morgan's systems employ antivirus technology to protect integrity of both the User's and your organization's data. The Pay Connexion servers use the UNIX® operating system, which is not susceptible to viruses found in other operating systems. The virus protection is signature-based and is updated nightly, or more frequently as necessary. Additionally, a dedicated team of IT security professionals, called the Computer Security Incident Response Team (CSIRT), is constantly monitoring vendor or industry advisories for reported threats, vulnerabilities, or incidents. CSIRT is responsible for communicating and resolving issues around the clock. Strict access control and physical security safeguards are implemented at both the primary and backup data centers to maintain a controlled, limited access environment for the areas supporting our Pay Connexion solutions. Our data is housed in government grade robust, firewall-protected, and secure Oracle databases linked to Sun Solaris servers using SSL 1024-bit encryption for security. Geographically dispersed secure primary and back-up data centers help ensure application readiness and availability. J.P. Morgan systems will meet or exceed the City's security requirements.			
T1.9.18	**Unauthorized Access Protection:** The system should protect against unauthorized access to data by persons and other software programs.	Describe how system provides security protection against unauthorized access to the database.	Expected
Please see our response to *Req # F501, Req# F518, and Req # T1.9.17* above.			
T1.9.20	**Security Transaction Log:** The application should provide a transaction log related to changes made to security (roles/groups/permissions).	Provide an example of the security transaction log provide by the application and explain how authorized users can access the log.	Expected
Please see our responses to *Req # F501 and Req # T1.4.9* above. Please see the sample Admin User Access Report in *Attachment 2* which provides details of Admin Users, Roles and Privileges.			
T1.9.21	**Specific User Lockout Capability:** To help enforce City's security policies, the solution should allow the application administrator to disconnect a particular user and to lock out a user during an active session.	Describe how the solution allows the application administrator to lock out a particular user and to disconnect a user during an active session.	Expected
Please see our responses to *Req # F501* above. Security Officers have the ability to temporarily remove an admin user's abilities to perform any/all administrative functions as well as to permanently disable an admin user's user ID.			
T1.9.22	**Login Attempt Threshold:** Authorized users should be able to define the number of login attempts allowed before a user account is locked and/or disabled.	Describe how authorized users can define the number of login attempts before a user account is locked and/or disabled.	Expected
The number of failed log-in attempts that is allowable before an admin user's log-in credentials are locked is not configurable by the City.			
T1.9.23	**Login Attempt Limitation:** The solution should log an event and alert the application administrator when a user exceeds login	Describe how the solution logs an event and alerts the application administrator when a user exceeds login attempts.	Expected

	attempts.		
Please see our response to *Req F507*. While Security Officers will not be automatically alerted when an admin user exceeds the allowable number of failed log in attempts before having log-in credentials locked, Security officers can confirm an admin user's locked status via the admin site.			
T1.9.24	**Automatic Inactivity Log Off:** The system should automatically log-off a user due to inactivity within a City-defined period.	Explain how inactivity time-out periods are defined. Describe what happens when an inactivity time-out is detected.	Expected
Inactivity on the Web and Admin channels in excess of a system defined time-out period will cause the browser to refresh, and present a time-out message. The payer/admin user must establish a subsequent session to access Pay Connexion. This reduces the risk of exposure of any data that was on the screen prior to the timeout as well as the risk of an unauthorized user performing functions after the authorized user left the browser without completing the session. The timeout period is not a configurable by the City, and is set system-wide at 20 minutes.			
T1.9.26	**Configurable Security Profiles:** The system should support the creation of security profiles/templates based on individual and group privileges.	Describe how authorized users can create security profiles to establish individual and group privileges.	Expected
Please see our responses to *Req # F501* above.			
T1.9.27	**Role Based User Groups:** The system should support to creation of user groups based on defined roles.	Describe how role based user groups can be created.	Expected
Please see our responses to *Req # F501* above.			
T1.9.29	**Generic Login Restriction:** The application should allow the Application Administrator to restrict generic logins.	Describe how the Application Administrator can restrict generic logins.	Expected
Please see our responses to *Req # F501* above. Security Officers can establish user IDs and initial passwords per City policy. Admin users are forced to revise their passwords upon initial log-in. Leading security practices dictate that users should not share log-in credentials.			
T1.9.31	**Concurrent Login Limitation:** The application should allow the Application Administrator to set the number of concurrent logins for a particular user on the same or on multiple workstations. The application shall generate an alert if a user attempts or exceeds this number.	Describe the methods to limit the number of concurrent logins for a user on the same or on multiple workstations. What are the alerting methods if this number is exceeded?	Expected
Please see our responses to *Req # T1.9.29* above.			
T1.9.35	**Audit Reporting:** The system should have the ability to produce readable audit reports for compliance reporting, audit reporting and security investigations.	Provide a sample report that shows a selected user, timestamp and what data was accessed.	Expected
J.P.Morgan maintains extensive logging and time stamped detail of user activity which may be used in audit or			

security investigative activities. In the event that the City requires such a log, this information may be obtained after an authorized request is submitted to the Pay Connexion Client Service team that will provide support during the contract term. Sufficient detail is provided to "recreate" a transaction experience for investigative purposes.			
T1.9.3 6	**Open Records Act Compliance:** The system should have the ability to allow public information requests for covered data. A security account shall be able to pull this data outside of administrative accounts.	Describe how the system would support the open records act.	Expected
Please see our responses to *Req #501 and Req # T1.6.3.*			
T3.9.3	**Security Vulnerability Remediation:** If high vulnerabilities are discovered during annual security assessments, they should be remediated within one month of discovery.	Explain how security vulnerabilities will be remediated at the ASP facility	Expected
If any security vulnerabilities are discovered, remediation will be prioritized accordingly. A dedicated team of IT security professionals, called the Computer Security Incident Response Team (CSIRT), is constantly monitoring vendor or industry advisories for reported threats, vulnerabilities, or incidents. CSIRT is responsible for communicating and resolving issues around the clock.			
T3.9.4	**Network Security Logs:** All network traffic traversing the proposed system's network should be logged, and logs be kept for a minimum of (10) days.	Explain the network security logging performed and monitored by your hosting facility.	Expected
J.P. Morgan's Computer Security Incident Response Team (CSIRT) coordinates all incident response, investigation, and escalation processes. Clients would be notified of any breach that directly impacts their data using our normal communication channels, which are handled by the Customer Product and Communications groups. Detailed information is confidential and proprietary to J.P. Morgan and not for public disclosure. In addition, J.P. Morgan has implemented an automated intrusion detection system that actively monitors the network perimeter and critical locations within the network. Alerts are sent to a central repository for review and escalation. Events are monitored and actioned accordingly by the firm's global Security Management Centers. The technology used is confidential and proprietary to J.P. Morgan and not for public disclosure.			
T3.9.5	**Session Encryption:** If sensitive data is to be protected, the solution should support a form of network session encryption.	Explain the types of session encryption supported.	Expected
Each session is secured using Secure Sockets Layer (SSL) with 128-bit encryption technology.			
T1.9.2 5	**Authorized Users with Expiration Dates:** The system may enable the creation of user IDs with a set expiration time/date.	Describe how authorized users can create user IDs with an expiration date and time. (i.e. for contractors and temps)	Desired
Please see our responses to *Req # F501 and Req # T1.9.21* above. Pay Connexion does not support time-limited admin user access privileges.			
T1.9.3 4	**Federated Authentication:** The proposed system may be capable of authenticating users through federated authentication technology.	Provide details of your support for federated authentication, and provide a list of technologies and methods supported.	Desired
Pay Connexion does support Single Sign-On functionality. The auto login allows billers to pass a Payer's			

username and password in the session transfer and log the payer into Pay Connexion, thus enabling billers to provide a seamless experience to their users. To use the Auto Login feature, billers must also use the Web Services API method Initiate Public/Admin session transfer types.

User Interface Requirements

Req#	Requirement Description	Required Response	Rating
T1.10.2	**Section 508 Compliance:** If the solution is web-based and usable by public citizens, it must be ADA and compliant with Section 508 of the Federal Rehabilitation Act.	Provide evidence of section 8 compliance for publicly accessible web interfaces.	Must Have
Throughout the payment process, the Pay Connexion application offers assistance to payers through context-sensitive online help. The site is compliant with section 508 of the Americans with Disabilities Act.			
T1.10.5	**Single Sign-on:** End users should not have to log in separately to different modules of the application. A single sign-on shall be all that is required.	Describe how system allows a user to sign on once to access the entire application according to their access rights.	Expected
Pay Connexion does support Single Sign-On functionality. The auto login allows billers to pass a Payer's username and password in the session transfer and log the payer into Pay Connexion, thus enabling billers to provide a seamless experience to their users. To use the Auto Login feature, billers must also use the encrypted session transfer.			
T1.10.11	**Configurable User Interface:** The system should provide a highly configurable user interface without requiring modification of program code.	Indicate how user screens and other user interface components may be customized by the City without requiring modification of program code.	Expected
Pay Connexion offers myriad configurable user interface features. Please see Biller Supplement User Interfaces in *Attachment 6* for specific detail regarding configurable options.			
T1.10.10	**Mobile Device Compatibility**: The application may provide Web functionality for wireless hand-held devices (WAP) as part of publicly accessible Web Service.	Describe your Web service's capability to present information to hand-held devices.	Desired
Pay Connexion supports a mobile payment channel. On an application-specific basis, registered payers may enroll via the web channel for mobile payments. When triggered by data submitted from the City, Pay Connexion will alert the payer via text message that a payment is due and provide the payer with the option to make a payment using the account that was designated at the time of mobile enrollment. Additionally, as long as the Mobile Device utilizes a supported web browser (Microsoft Internet Explorer version 6.0, 7.0, 8.0 or Firefox 3.0, 3.5 or Google Chrome 3.0, or Safari 4 or 5) and/or DTMF telephone the Pay Connexion Web and/or IVR channels (respectively) may be utilized.			

IMPLEMENTATION REQUIREMENTS

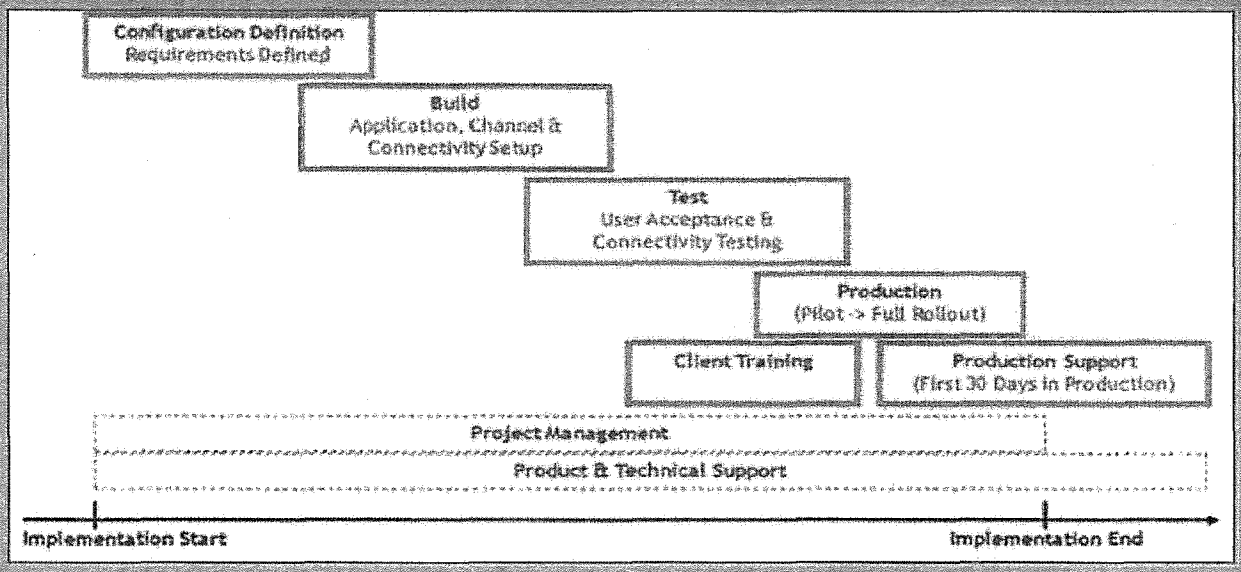
The implementation requirements describe the project management resources, processes, documentation and training that ensure effective system implementation and successful

transition to operations. Vendors shall respond to the implementation requirements by providing the documentation, plans, and/or other requested information as indicated.

Project Management

Req#	Requirement Description	Required Response	Rating
IMP1	**Project Management Methodology:** The vendor should provide evidence of a mature project management methodology.	Describe the proposed methodology including how it will be used in this project. Provide evidence that this approach has resulted in successful projects in the past.	Expected

J.P. Morgan uses the PMI methodology, a proven approach to setup, implementation, and testing of Pay Connexion. Pay Connexion has a dedicated and experienced Implementation and Service group which specializes in bringing clients online quickly and efficiently. Implementing Pay Connexion has five phases: Configuration, Build and Setup, Testing, Training and Production, and Production Support.



J.P. Morgan has completed numerous complex implementations using this proven methodology, including:

- An IVR channel implementation for a major utility company that included custom interfaces and convenience fee programs to meet complex regulatory requirements
- An IVR and Web implementation for 3 of the top 4 big Automobile Manufacturers
- A Web channel implementation for a major pharmacy management company that included segmentation to match over twenty different business units

We have incorporated the best practices learned from these and other major implementation projects into our Implementation Project Plans.

IMP2	**Project Management Plan:** The vendor should provide evidence of a mature project management methodology.	Describe the tasks, milestones and resources required for each phase of the project schedule.	Expected

The PCX implementation timeline is based on a 16 week implementation standard. The timeline varies based upon the selected scope and feature set complexity. The most significant timeline drivers are often on the client side: Client availability, client decision making during requirements definition, and client resource dedication and priority given to testing. Given the client-side dependencies and unknowns about specific configuration requirements, the sample project plan is provided in *Attachment 7* for illustrative purposes only, without specific commitment regarding the task line and/or task durations.

Pay Connexion has dedicated Implementation Managers who run weekly planning, status, and issue tracking meetings, in addition to day-to-day support.

We employ the J.P. Morgan Delivery Process, our standard project management methodology, to implement Pay Connexion. This methodology has been in place for the past ten years and has proven over and over again as a sound discipline that delivers projects on time and within budget. The J.P. Morgan Delivery Process delivers Pay Connexion and other A/R interfacing solutions hundreds of times a year.

In addition to leveraging the J.P. Morgan Delivery Process, we offer a unique approach to setup, implementation, and testing of Pay Connexion. Our experienced Implementation and Service group specialize in bringing clients online quickly and efficiently. Bringing up a Pay Connexion application has four primary phases:

1. Educate and Gather (Configuration Requirements Definition and Solution Design)
2. Configure and Test (Application Build)
3. Correct, Review, and Train (User Acceptance Testing)
4. Finalize and Release (Production Activation)

Initiating the implementation project for each application requires the submission of Statement of Work document which outlines at a high-level the desired feature set for the subject application.

Once the project is kicked off, the initial phase of the implementation process includes providing overview training to the primary members of the City project team to insure the team has a good understanding of the overall application and process flow. We then begin a detailed requirements gathering process, where we work with the City to define all Pay Connexion functional requirements and the detailed operating flow. The design of each City application will be the result of configuration requirements definition meeting(s). During this meeting (or series) the assigned Implementation Manager will facilitate an exchange in which the City project team (comprised of both "business" and "technical" participants) will be interviewed about the application vision, objectives and constraints and be educated on in-scope features and relevant options. The Implementation Manager will bring to bear deep subject matter expertise and experience with other similar applications in making recommendations. Configuration design is done in parallel with requirements definition and is confirmed prior to the Build phase of the project. We will ask the City to sign-off on this requirements document.

Using these requirements, your Pay Connexion Implementation Manager will configure and build your Pay Connexion web, IVR, and/or Administrative channels. This build will include your desired branding, payment options, business rules, and other City -specific needs.

Test Plan

Req#	Requirement Description	Required Response	Rating
IMP3	**Testing Methodology Model:** The vendor should provide a detailed model as to how products and services are tested.	Provide a detailed explanation of your testing methodology and the process that is used to create your test plans. Explain how this approach will be used in this project.	Expected

Once built, the City's application will undergo three User Acceptance Testing phases:

Phase 1 – Presentation Testing

- Review the web presentation and branding, making adjustments as necessary
- View the administrative site for reporting
- View the administrative site for CSR payment support presentation, if applicable, making adjustments as necessary

Phase 2 - Functional/Integration Testing

- All Web components locked down, including translated components
- Test the creation of all files to be sent for processing in the Pay Connexion system; all coding is complete for file creation along with the file transmission scripting to transmit the files
- Test the receipt of all files and their processing in back-end system; all coding is complete to process all files along with the file transmission scripting to either pick up or receive the files
- Make payments and review through the administrative site
- Review all reports through the administrative site
- Develop all training materials for your Customer Care Center

Phase 3 – End-to-End Testing

- Receive all Pay Connexion files daily through the predefined file transmission protocol and process through back-end systems
- Make payments (simulate production)
- Review payments through the administrative site
- View all reports on the administrative site
- Train all customer CSR's on the application (if applicable)

Once the above User Acceptance Testing phases are complete, and the City has signed off on the approval to activate, various due diligence steps are taken prior to activation including an internal review of the entire application and supporting documentation, and activation interview/call with the City's project team.

J.P. Morgan will then launch the City's application into production. Post activation validation is then executed including making live pilot payments in the production environment to ensure proper processing and settlement of production payments. These pilot payments can later be refunded if needed.

At this point, the application is ready to be opened to the City's payer base for general availability. For the first 30 days, the implementation team will continue to monitor the application and usage patterns. After 30 days, the application will move into the Operations Practice Management group. This group will provide ongoing support, metrics, and reviews, and is available 24x7.

IMP4	**Sample Test Plans:** The vendor should provide a minimum of two (2) recent test plans.	Provide samples of recent test plans that clearly show the process used for testing and system test results.	Expected

Please see our response to *Req #IMP2* above.

Actual project plans from prior clients' projects cannot be provided due to client confidentiality policies, but are similar to the illustrative sample project plans in terms of the high-level task-line, and task durations given a degree of variability to account for differences in application configurations and client side execution.

IMP5	**Test Plan:** The vendor should provide a detailed test plan specific to the needs of the City.	Provide a detailed test plan that describes how the system will be tested including interfaces, performance, migration and	Expected

		user acceptance.	
Please see our response to *Req #IMP2 and Req # IMP4* above. Please refer to the sample project plan, provided as *Attachment 7*, for details on the testing phase of implementation. This project plan is for illustrative purposes only without specific commitment regarding the task line and/or task durations. During Implementation, the assigned Implementation Manager will provide a detailed Testing Checklist that is tailored to the City's application configuration specifics. This checklist provides the City with specific guidance at each step of the User Acceptance Testing phase of Implementation.			

Implementation and Integration

Req#	Requirement Description	Required Response	Rating
IMP6	**Implementation Plan:** The vendor should provide a detailed breakdown of steps/timeframes required to implement product and/or services.	Provide an implantation plan that details steps and timeframes required to implement specific products and services.	Expected
Please see our response to *Req #IMP2, Req # IMP4 and Req # IMP5* above. Given the client-side dependencies and unknowns about specific configuration requirements, the sample project plan is for illustrative purposes only without specific commitment regarding the task line and/or task durations. A tailored project plan will be provided once project scope and configuration requirements are defined in greater detail.			
IMP7	**Implementation Personnel:** The vendor should provide qualified and experienced onsite project management and technical resources.	Describe the qualification and experience of onsite personnel including sample resumes from personnel that may be deployed to the City's site.	Expected
The Pay Connexion Service Delivery Unit consists of Implementation Project Managers that are extensively trained on and dedicated to Pay Connexion. This team is managed by Patricia Carroll, Vice President, Pay Connexion Implementation Project Manager Lead. Patty has worked with Pay Connexion for 9 years and has 20 years of Onboarding, Operations, and Product Support experience. She also has significant implementation experience across industries including financial, government, utility, and insurance sectors. Patty is fully aware of the associated regulatory and customer experience issues that need to be addressed to deliver a successful solution on schedule. Patty holds a Bachelor of Arts degree in History from St. Xavier University.			
IMP8	**Integration Services:** The vendor should provide the ability to deliver onsite implementation services.	Describe the specific onsite implementation services that are offered. The City's preference is that these services are offered from local or regionally based locations.	Expected
Please see our response to *Req #IMP7* above.			
IMP9	**Transition Plan:** The Vendor should provide a plan to transition and "go-live" with the new system in their proposal.	Describe how the "go-live" will be executed and how affected stakeholders will be prepared for this transition. Include any transition/cut-over plan recommendations that may be relevant to this project.	Expected
Please refer to our response to *Req# IMP1 Req# IMP2 Req# IMP3 Req# IMP4 and Req# IMP5* for a detailed description of the implementation process.			

A sample project plan is provided in *Attachment 7*. Additional detail regarding Roles and Responsibilities during each phase of Implementation including activation the will be provided during the Project Kickoff, and throughout the project as needed during weekly status calls. Throughout the project as more detail is learned/confirmed the City's "current state", "target state", Pay Connexion configuration, User Acceptance Testing progress and more the Implementation Manager will support the City with recommendations relevant to the transition/cutover.

IMP10	**Successfully Completed "go-lives":** The Vendor should provide samples of past implementations that were completed with projects of similar size, scope and complexity.	Describe past "go-lives" that were completed successfully including any pertinent lessons learned and best practices.	Expected

Each of the following multi-application Public Sector projects were similar in size, scope and complexity to the project outlined by the City of Austin. Best practices that were highlighted from each of these projects include:

While each Department-centric project will likely involve Department personnel, it is very helpful for some core project participant(s) to be engaged across all projects. This continuity minimizes the time that the City spends learning the Pay Connexion features, terminology, etc. and better enables the City to utilize Configuration Requirements in common to optimal degree. This approach reduces the need for each Department to "re-invent the wheel".

It is essential for all impacted stakeholders to be engaged with the project from the Kickoff and remain actively engaged as needed. This not only includes business and IT perspectives, but also may involve the City's third party providers. If some perspectives are not represented during the Kickoff and Configuration Requirements Definition phases of the project, then there is a risk of re-work.

Table 14 - Implementation Refrences

City of Grand Rapids, Michigan	
Point of Contact	Al Mooney
Contact Title	City Treasurer/Treasury Director
Address	City of Grand Rapids Ste. 220 300 Monroe Ave. NW Grand Rapids MI 49503
Phone Number	(616) 456-3285
Contact's e-mail address	amooney@grcity.us
Work Performed	City of Grand Rapids utilizes Pay Connexion Web and IVR in English and Spanish for multiple applications, including property taxes, water bills, parking violations, and miscellaneous receivables and uses On Site Card Payments with Convenience Fees for various payment types.

Erie County, New York	
Point of Contact	Lorne Steinhart
Contact Title	Acting Comptroller, County of Erie, Office of the Comptroller
Address	95 Franklin Street, Room 1100 Buffalo, New York 14202-3971
Phone Number	Tel: 716-858-8400
Contact's e-mail address	Lorne.Steinhart@erie.gov

Work Performed	Erie County utilizes Pay Connexion Web for multiple applications, including property taxes, parks and recreation, environmental health, public works, and weights and measures and uses On Site Card Payments with Convenience Fees for various payment types.

City of White Plains, New York	
Point of Contact	Nino Pennacchio
Contact Title	Comptroller
Address	255 Main Street White Plains, NY 10601
Phone Number	(914) 422-1397
Contact's e-mail address	npennac@ci.white-plains.ny.us
Work Performed	City of White Plains utilizes Pay Connexion Web for multiple applications, including property taxes and utilities.

Training and System Documentation

Req#	Requirement Description	Required Response	Rating
IMP11	**Training Plan:** The Vendor should provide a detailed training plan targeted for specific user groups.	Describe how training plan will address the needs of various user groups (e.g. system administrators, financial administrators, technical resources).	Expected

Late in the testing phase and shortly before launch, we will execute training for your key personnel.

The "Train the Trainer" session(s) for your key staff is complemented by:

- Product documentation
- Sophisticated context sensitive online Help to provide users with quick instructions
- Unlimited access to online interactive training for employees
- Standard administrative user functionality: generating reports, assisting customers and editing transactions
- General consumer functionality: making payments, adding payment accounts and viewing historical transactions
- Problem resolution for the payment applications

You are provided with an e-Learning tool during the testing phase of the implementation and made available through the remaining contract period to assist the administrative users. The e-Learning application includes:

- An overview of the Internet application
- An overview of how the customer interacts with the application

The self-taught, Web-based e-Learning training can be completed individually or in a group setting. The e-Learning application is broken down into small component, so that if administrative users have specific questions about a topic, they can click through that topic without having to view the entire session. The entire e-Learning training can be completed within two to three hours.

At no additional cost, we can provide instructor-led training as needed either onsite or through the Web to supplement e-Learning. The instructor-led training follows the "train the trainer" approach.

Upon contract award, we provide you with the Biller Connectivity Reference Guide, which outlines the file transmission process and the connectivity guidelines. Additionally, we provide the Functional Specification Document, which defines the features and functionality of the Internet, IVR, and Administrative applications. These documents are also available in electronic format. J.P. Morgan has a complete suite of printed and electronic training material as well as a proven "train the trainer" based methodology designed to enable the City's personnel to rapidly gain expertise with the Pay Connexion solution. Additionally, our implementation specialists will work with the City's personnel during the period immediately after "going live" to ensure they are completely comfortable with all aspects of the solution.			
IMP12	**Training Materials:** The Vendor should provide training materials that can be adapted for use by City staff to conduct end user training.	Describe what kinds of training materials will be provided and how these can be modified for use by City staff to conduct user training.	Expected
J.P. Morgan has a complete suite of printed and electronic training material as well as a proven "train the trainer" based methodology designed to enable the City's personnel to rapidly gain expertise with the Pay Connexion solution. Additionally, our implementation specialists will work with the City's personnel during the period immediately after "going live" to ensure they are completely comfortable with all aspects of the solution.			
IMP13	**Ongoing Training Recommendations:** The Vendor should submit recommendations on how to conduct ongoing training for new users and training for future upgrades.	Describe the process that will be used to keep users up to speed on new features and system upgrades.	Expected
Our approach includes "train the trainer" and allows the City adapt standard Pay Connexion documentation/content for its own unique purposes to make the City independent with respect to ongoing training needs. If additional "train the trainer" training is desired, the City may requests this through the Client Service organization. Prior to the release of new features, Release Notes will be distributed to personnel as designated by the City. If the City initiates any Change Request projects to either modify its application configuration(s) or take advantage of new configurable features, then training will be provided during the Change Request project as appropriate for the incremental functionality.			
IMP14	**Proposed System Architecture:** The Vendor should provide documentation of proposed system architecture with complete data element dictionary.	Provide detailed architecture diagrams that clearly describe integration points between the vendor system and City applications.	Expected
Please see our response to *Req #T3.10.1.*			
IMP15	**Maintenance/Operations/User Manuals:** The Vendor should provide documentation for each module of system software.	Provide detailed user manuals that address each module of the system software.	Expected
Please see our response to *Req #T3.10.1 and Req # IMP11.*			

SUPPORT AND ONGOING SERVICE

Req#	Requirement Description	Required Response	Rating
SUP1	**Support Model:** The Vendor should provide their approach and availability as it pertains	Describe the model that is used to support the system.	Expected

to product and/or service support.

J.P. Morgan will utilize the following approach with respect to support:

Tier I Support	Telephone-based support whereby Customer's Payors access a Customer support representative for assistance on Payor-related issues specific to the Services during regularly scheduled Payor service hours.
Tier II Support	Telephone-based support whereby Customer's support representative can call a Bank support representative for assistance on Payor-related issues specific to the Services.
Tier III Support	Telephone-based customer support whereby Bank support representatives escalate Service problems to internal technical resources for issue resolution.

Bank will only provide Tier I support in cases where Customer requests assistance as part of the IVR channel service (roll-out operator support). Tier II customer service representatives resolve those calls for which Tier I staff require assistance. Tier II requests may require additional internal/external investigation to be performed by dedicated staff. Tier III support representatives will be responsible for analysis and resolution of technical or other system-related problems. Tier III support will be staffed and supported by Bank technical or knowledge subject matter experts. Customer will be able to contact the bank via toll-free number or email address to be provided during Implementation for Tier II support, technical issues, or to report system interruptions.

PRODUCTION EXPECTATIONS

When Customer's Pay Connexion system is in production, Bank will be responsible for the following in addition to the service levels identified herein:

- Housing the system in a secure environment and adherence to regulatory and audit requirements of this kind of payment system. Security is defined as utilizing proper encryption and access control standards.
- If using Bank Call Center, authentication of users as they enter the system pursuant to Bank policies and procedures.
- Archival of pre-registration file for 2 weeks after acceptance for possible retrieval.
- Initiation of the RTPC and API transaction in the appropriate format in a timely manner. (Optional Service)
- Processing payments through the appropriate payment channels as configured during set up.
- Making data available for reporting queries initiated through the Pay Connexion Administrative system for two years standard
- Send emails as indicated in the Functional Specification to either internal resources or to the Payer directly based on events in the payment process.
- Pre-Registration File Processing as described in the SLA herein
- Next Day Remittance Processing as described in the SLA herein
- Same-Day Processing Remittance Processing as described in the SLA herein

When Customer's Pay Connexion system is in production, Customer will be responsible for the following:

- Providing daily updates to the Pre-Registration file (if selected) for retrieval by Bank by 9:00PM ET.
- Retrieve the remittance file delivered each Business Day by Bank
- Ensure that all data required in the session transfer, as part of the Pre-Registration file or API, is made available as appropriate for processing payments. If a data element is missing or is sent in plan text when it is expected to be encrypted the session will error for the Payer.
- Notify JPMC in advance of infrastructure changes that may impact session transfer, email confirmations,

FTP transmissions, and successful RTPC receipt.			
SUP2	**Support and Maintenance Plan:** The Vendor should provide a comprehensive plan describing how the system and its connection to the City's suite of applications will be supported and maintained.	Provide a detailed five year support and maintenance plan including: How to contact the Vendor Vendor support team availability Service levels Software/hardware is supported Warranty information Information about enhancements and upgrades	Expected
Please see our response to Req # SUP1, Req # T3.3.3, and T1.1.7. Prior to each major release, Release Notes will be delivered to the City's designated personnel outlining the features being deployed in the release.			
SUP3	**Sub-Contractors:** The Vendor should have clear roles/responsibilities and accountability with any sub-contractors connected with the system.	Describe the roles/responsibilities and accountability (i.e. SLAs) with any sub-contractors connected with the system, including its implementation and support.	Expected
J.P. Morgan does not utilize third parties or subcontractors in developing, implementing, operating or supporting Pay Connexion.			
SUP4	**Continuous Improvement:** The Vendor should provide information concerning planned releases and roadmaps to expand and improve product and service offerings.	Describe any planned releases and roadmaps associated with expanding or improving the system in the future.	Expected
There are typically three to five product feature releases annually, each of which includes functionality which is developed internally and tested extensively. Minor/Maintenance releases may also be deployed throughout the year. Prior to each major release, Release Notes will be delivered to the City's designated personnel outlining the features being deployed in the release.			

COST

Req#	Requirement Description	Required Response	Rating
COST 1	**Transaction Fees:** The vendor must detail the total cost per transaction of using their system.	Describe the total cost per transaction associated with using the system including any tiered transaction discounts based on quantity or transaction amount.	Must Have
Please refer to the Pay Connexion Fee Schedule in Exhibit C (Pay Connexion Standard Service Level Agreement).			
COST 2	**Merchant Processor Fees:** The Vendor must detail any fees associated with using the proposed merchant processor. (Only applies to prospective vendors bringing their own merchant processor).	Detail any and all fees associated with using the Vendor's merchant processor including any tiered transaction discounts based on quantity.	Must Have
Please refer to the Pay Connexion Fee Schedule in Exhibit C (Pay Connexion Standard Service Level			

Agreement).			
COST 3	**Setup/Termination Fees:** The Vendor must detail any costs associated with initial system set-up, configuration or termination of the system.	Detail any setup, configuration or termination fees associated with the system.	Must Have
Please refer to the Pay Connexion Fee Schedule in Exhibit C (Pay Connexion Standard Service Level Agreement).			
COST 4	**Monthly and/or Annual Fees:** The Vendor must detail any costs associated with ongoing recurring costs (Transaction fees are separate).	Describe any recurring monthly or annual fees associated with the system.	Must Have
Please refer to the Pay Connexion Fee Schedule in Exhibit C (Pay Connexion Standard Service Level Agreement).			
COST 5	**Support and Maintenance Fees:** The Vendor must describe any support costs or system maintenance/upgrade fees.	Describe any support costs (per incident or other) or system maintenance/upgrade fees associated with the system.	Must Have
Please refer to the Pay Connexion Fee Schedule in Exhibit C (Pay Connexion Standard Service Level Agreement).			
COST 6	**Storage Fees:** The Vendor must provide any fees associated with data storage.	Describe any fees associated with storage of real time or archived data. Include any tiered discounts or cost structures based on type and amount of data storage.	Must Have
Please refer to the Pay Connexion Fee Schedule in Exhibit C (Pay Connexion Standard Service Level Agreement).			
COST 7	**Interface Fees:** The Vendor must provide integration costs to integrate with existing City financial system (CGI Advantage) and department billing/sales systems or customize product/service to meet City requirements.	Provide a detailed explanation of costs associated with integration and customization. Our preference is that this cost is based on a per hour fee.	Must Have
Please refer to the Pay Connexion Fee Schedule in Exhibit C (Pay Connexion Standard Service Level Agreement).			
COST 8	**Years 2 through 5 Fees:** The Vendor must provide an additions or reductions to any fees after year 1.	Describe any additions or reductions to any portion of the fee schedule for years 2 through 5.	Must Have
Please refer to the Pay Connexion Fee Schedule in Exhibit C (Pay Connexion Standard Service Level Agreement).			

Exhibit B
Pay Connexion Service Terms

PAY CONNEXION[SM] SERVICE TERMS L JPMORGAN CHASE BANK, N.A.

V06-28-11

1. Service and Service Terms.

These Service Terms apply to **JPMorgan Chase Bank, N.A. ("Bank")** Services for Pay Connexion[SM] provided to **City of Austin ("Public Sector Entity")**. Bank's account documentation, including account terms and conditions governing the operation of business accounts and services as well as other applicable service terms, (collectively, "**Account Documentation**"), are incorporated into these Service Terms by this reference. Capitalized terms used herein and not otherwise defined shall have the same meaning specified in the Account Documentation.

2. Definitions.

2.1 "API" or "Application Programming Interface" means an interface implemented by a software program that facilitates interaction between the Service and Public Sector Entity's software programs. For example, API includes a message request sent from the Service to another software program and a message response from one software program back to the Service.

2.2 "Authorized User" means a designated employee or agent of the Public Sector Entity.

2.3 "Call Center" means Bank's customer service operations, as applicable.

2.4 "Card" is an account, or evidence of an account, authorized and established between a Payor and a Payment Brand, or representatives or members of a Payment Brand that Public Sector Entity accepts from Payors as payment for a good or service. Cards include, but are not limited to, credit or debit cards, stored value cards, loyalty cards and electronic gift cards.

2.5 "Convenience Fee(s)" means a charge to a Payor's Card or checking or savings account for the convenience of using the payment channels offered via the Service, which includes the Internet, Point-of-Sale, IVR, Call Center, and API, as applicable, where such charge is collected by Bank, including as agent on behalf of Public Sector Entity, if applicable.

2.6 "Image File" means, if applicable, an electronic file containing a summary or detail Statement or payment information.

2.7 "IVR" means the Bank-provided interactive voice response system.

2.8 "Merchant Processor" means the provider of services necessary to authorize, process and settle, as applicable, Payors' Card transactions contemplated hereunder.

2.9 "NACHA" means the National Automated Clearing House Association.

2.10 "NACHA Rules" means the operating rules and guidelines of the National Automated Clearing House Association.

2.11 "Payment Brand" is any payment method provider whose payment method is accepted by Merchant Processor for processing, including, but not limited to Visa, U.S.A., Inc., MasterCard International, Inc., Discover Financial Services, LLC and other credit and debit card providers, and debit network providers. Payment Brand also includes the Payment Card Industry Security Standards Council.

2.12 "Payment Brand Rules" are the bylaws, rules, and regulations, as they exist from time to time, of or required by the Payment Brands.

2.13 "Payor" means consumer or business customers of Public Sector Entity who access the Point-of-Sale, IVR, Call Center or the Internet, as applicable, to initiate payments to Public Sector Entity. Where applicable, Payor also means the person or entity to whom a Card is issued or who is otherwise authorized to use a Card.

2.14 "Payor Information" means information related to a Payor or the Payor's Card, that is obtained by Public Sector Entity or Bank from the Payor's Card, or from the Payor solely in connection with his or her use of a Card (e.g., a security code, a PIN number, credit limits, account balances, or the Payor's zip code when provided as part of an address verification system). Without limiting the foregoing, such information may include the Card account number and expiration date, the Payor's name or date of birth, PIN data, security code data (such as CVV2 and CVC2), and any data read, scanned, imprinted, or otherwise obtained from the Card, whether printed thereon, or magnetically, electronically, or otherwise stored thereon. For the avoidance of doubt, the data elements that constitute Payor Information shall be treated according to their corresponding meanings as "cardholder data" and "sensitive authentication data" as such terms are used in the then current Payment Card Industry Data Security Standards ("PCI DSS").

2.15 "Point-of-Sale" or "POS" means electronic payment system used in Card-present transactions to verify and process Card information.

2.16 "Public Sector Entity Website" means a web site owned or operated by or on behalf of Public Sector Entity.

2.17 "Rules and Regulations" means the NACHA Rules, the Payment Brand Rules, or other applicable association or clearinghouse rules, the Security Standards, and all other applicable laws, regulations and industry rules, each as amended from time to time.

2.18 "Security Standards" are all rules, regulations, standards or guidelines adopted or required by the Payment Brands or the Payment Card Industry Security Standards Council relating to privacy, data security and the safeguarding, disclosure and handling of Payor Information, including but not limited to the PCI DSS, Visa's Cardholder Information Security Program ("CISP"), Discover's Information Security & Compliance Program, American Express's Data Security Operating Policy, MasterCard's Site Data Protection Program ("SDP"), Visa's Payment Application Best Practices ("PABP"), the Payment Card Industry's Payment Application Data Security Standard ("PA DSS"), MasterCard's POS Terminal Security program and the Payment Card Industry PIN Entry Device Standard, in each case as they may be amended from time to time.

2.19 "Service(s)" means the specific service(s) provided by Bank more specifically described in the service level agreement ("Service Level Agreement" or "SLA") attached hereto as Exhibit C and incorporated by reference, the statement of work ("Statement of Work") and the implementation questionnaire that will be completed by Public Sector Entity and Bank subsequent to execution of the Service Terms. The Services include a payment solution that allows Payors to initiate payments to Public Sector Entity via the Internet, Point-of-Sale, IVR or Call Center; access to the Technology; reporting and analysis capabilities, and if applicable, electronic statement presentment.

2.20 "Service Start Date" means the date the Public Sector Entity Website, Point-of-Sale, IVR or Call Center application, as applicable, is activated.

2.21 "Statement" means, if applicable, a bill or invoice, as applicable, or comparable request for payment, prepared and sent to Payors by or on behalf of Public Sector Entity.

2.22 "Technology" means Bank's (or its licensor's) Point-of-Sale, IVR, API and/or web-based applications, as applicable, which have been designed to facilitate Payor-initiated payments relating to various transactions entered into between Payors and Public Sector Entity, via telephone to Call Center or IVR, Point-of-Sale, or the Internet, using as applicable, Cards, or via automated clearing house ("ACH") and may include customer service support, reports, software, and software tools, user interface designs, and documentation, and any derivatives, improvements, enhancements or extensions thereof.

2.23 "Term" shall mean the Initial Term and any Renewal Term(s) as defined in Section 8.1, unless earlier terminated in accordance with Section 8.2.

3. Responsibilities; Suspension/Cancellation of Service.

3.1 Public Sector Entity Responsibilities. Public Sector Entity agrees to, at its sole expense and consistent with the Rules and Regulations: (a) maintain the Public Sector Entity Website, IVR and API, as applicable, as well as the actual links and session transfer capabilities; (b) maintain the URLs to which Payors are returned after completing a payment transaction for the Services via the Internet; (c) provide Bank with all information reasonably necessary to setup or establish the Service on Public Sector Entity's behalf, including but not limited to completing the Statement of Work and implementation questionnaire documentation and using commercially reasonable efforts to ensure its vendors, if applicable, cooperate fully with Bank to achieve inter-operability of the Technology and Services with Public Sector Entity's or its vendors hardware, (d) maintain the confidentiality of any passwords, codes, digital certificates, security devices and related instructions for use of the Services, and if Public Sector Entity believes or suspects that any such information or instructions have been accessed by unauthorized persons, Public Sector Entity shall promptly notify Bank and advise Bank as to the effect of the security breach and the corrective actions to be taken to restore or verify security; (e) advise each Authorized User of his or her obligations under these Service Terms and of the license restrictions set forth herein; (f) if applicable, provide Payors with all required disclosures pursuant to the Rules and Regulations and as otherwise agreed to by the parties, including but not limited to, where Public Sector Entity is accepting POS Transactions, ensuring that all required disclosures relating to Convenience Fees are made by Public Sector Entity to each Payor at the point-of-sale (Public Sector Entity shall certify its compliance with the disclosure requirements in writing to Bank on an annual basis); (g) if applicable, provide proper attribution of the Technology and Services to Bank as determined by Bank; (h) provide appropriate and sufficient data to authenticate Payors, including but not limited to delivery of data that will be (1) validated by the Service when a Payor is attempting access, (2) used to perform the authentication of the Payor when the Service is not providing the authentication; and (3) used to validate the Payor after a successful session transfer for ACH transactions; (i) maintain the confidentiality of any passwords, codes, digital certificates, security devices and related instructions for use of the Services, and if Public Sector Entity believes or suspects that any such information or instructions have been accessed by unauthorized persons, Public Sector Entity shall promptly notify Bank and advise Bank as to the effect of the security breach and the corrective actions to be taken to restore or verify security; (j) be responsible for all chargebacks, except for chargebacks of Convenience Fee payments where charged and collected by, and settled to, Bank; (k) enter into a merchant processing agreement with a Merchant Processor acceptable to Bank ("Merchant Agreement");; and (l) pay all fees and charges applicable to the Service. All payments to the Bank shall be in full, without set-off or counterclaim and free of any deduction or withholdings related to any tax or other claim. All services required by Public Sector Entity not listed in a Statement of Work will be charged at Bank's standard prices. All requests for additional development or changes will follow the standard Pay Connexion change request process. Bank may impose, charge and adjust

fees associated with the Service and included in Exhibit D, including but not limited to, any applicable maintenance fees with 30 days notice to Public Sector Entity. Public Sector entity shall not: (A) engage in spamming, mail bombing, spoofing or any other fraudulent, illegal or unauthorized use of the Services; (B) alter, translate, create derivative works from, reverse engineer, disassemble or decompile the Technology or Services; (C) knowingly introduce or transmit through the Technology or Services any virus, worm, software lock, drop dead device, Trojan-horse routine, trap door, back door, timer, time bomb, clock, counter or other limiting routine, instruction or design or any other codes or instructions that may be used to access, modify, delete, damage, disable or prevent the use of the Technology or Services or other computer systems of Bank; (D) remove, obscure or alter any copyright notice, trademarks or other proprietary rights notices affixed to or contained within the Technology or Services without Bank permission; or (E) engage in or allow any action involving the Technology or Services that is inconsistent with these Service Terms and all functional specification documents that are or will be provided to Public Sector Entity by Bank.

3.2 Bank Responsibilities Associated with the Services. Bank agrees, consistent with the Rules and Regulation, that it will not (a) engage in spamming, mailbombing, spoofing or any other fraudulent, illegal or unauthorized use of the Services; or (b) knowingly introduce or transmit through the Technology or Services, any virus, worm, software lock, drop dead device, Trojan-horse routine, trap door, back door, timer, time bomb, clock, counter or other limiting routine, instruction or design or any other codes or instructions that may be used to access, modify, delete, damage, disable or prevent the use of Public Sector Entity's computer system.

3.3 Withdrawal of Access/Suspension of Service. Bank may, in its reasonable discretion, instruct Public Sector Entity to terminate access to any Authorized User or individual and Public Sector Entity agrees to promptly comply with such instructions. Bank reserves the right to deny, suspend or revoke access to the Services, in whole or in part, if Bank believes Public Sector Entity and/or its Authorized Users are in breach of these Service Terms or are otherwise using or accessing the Services inconsistent with the terms and conditions hereof. Further, Bank shall have the right to suspend the Service immediately in the event of an emergency or in the event of force majeure.

4. Payment Processing.

4.1 ACH Processing. Bank will initiate ACH entries to the checking or savings accounts of Payors who opt to pay using ACH transactions. Terms used herein but which are not defined in these Service Terms or the Account Documentation, have the meanings given those terms in the NACHA Rules. Public Sector Entity (as Originator) and Bank agree to be bound by the NACHA Rules in effect from time to time and shall comply with same. Public Sector Entity agrees not to close the account(s) designated as Public Sector Entity's settlement account (as used herein, individually and collectively, "Settlement Account"), which Settlement Account shall be at Bank, without giving Bank at least five (5) Business Day's prior written notice and substitution of another Settlement Account. As used herein, "Business Day" is defined as Monday through Friday, excluding Federal Reserve Bank holidays. Public Sector Entity authorizes Bank to initiate electronic debit and credit entries and adjustments to the Settlement Account without respect to the source of any monies in the Settlement Account. This authorization shall remain in full force and effect until termination of these Service Terms. Bank shall not be responsible or liable for any delays in receipt of funds or errors in Settlement Account entries caused by Public Sector Entity, Payors or third parties. In preparing and transmitting ACH entries, Bank may rely upon all information and data provided to it via the Service for any Payor, and Bank shall have no responsibility or liability for the inaccuracy or invalidity thereof.

4.2 Card Processing. Payor payments generated pursuant to the terms of these Service Terms from Card transactions will be tendered to Merchant Processor.

4.3 Convenience Fees. (a) Public Sector Entity instructs Bank as follows with respect to all Convenience Fees charged by, collected by and settled to Bank: (i) all Convenience Fees will be submitted by Bank to the Merchant Processor or through the ACH Network, as applicable, (ii) all evidence and electronic record of a sale or lease transaction ("Sales Data") representing payment by use of a Card or of a refund/credit to a Payor will be submitted by Bank on behalf of Public Sector Entity to the Merchant Processor or through the ACH Network, as applicable, (iii) all Merchant Processor processing fees, chargeback fees, funds transfer fees, interchange fees, dues, access, connectivity, and assessment fees, or other fees that may apply to submission of Convenience Fees and Sales Data shall be paid by Bank, except where the submission includes only Sales Data, in which case such fees shall be paid by Public Sector Entity(iv) all chargebacks, returns and similar charges related to Sales Data shall be paid by Public Sector Entity, (v) all chargebacks, returns and similar charges related to Convenience Fees shall be paid by Bank, (vi) settlement funding for Convenience Fees will be paid by Merchant Processor directly to Bank or an account designated by Bank, (vii) settlement funding for Sales Data will be paid by Merchant Processor directly to the Settlement Account, and (viii) Bank may change the Convenience Fee being charged at any time with 30 days written notice to the Public Sector Entity. (b) For all Convenience Fees charged by Public Sector entity, collected by Bank on behalf of Public Sector and settled to Public Sector Entity, Public Sector Entity shall pay all Merchant Processor processing fees, chargeback fees, funds transfer fees, interchange fees, dues, access, connectivity, and assessment fees, or other fees that may apply to submission of Convenience Fee and Sales Data, and all chargebacks, returns and similar charges related to Convenience Fees and Sales Data.

5. Statements (If Applicable: Statement Presentment is an optional service. This Section 5 will apply only where Public Sector Entity and Bank have documented acceptance of the Statement Presentment Service in an SOW , implementation questionnaire, or otherwise in writing).

5.1 Statement Presentment

(a) At an agreed upon time following each billing cycle, Public Sector Entity shall electronically transmit to Bank an Image File containing .pdf images of the Statements they wish to have presented. They will also pass this image identification in the Pre-Registraion file where it will be associated it with a Payor. Bank shall store the image on-line for 18 months. Bank shall have no obligation to act upon any Image File it is unable to verify.

(b) Public Sector Entity shall be responsible for the accuracy, adequacy and proper form of all Image Files and other data and information supplied by Public Sector Entity to Bank and Public Sector Entity shall notify Bank of any error or discrepancies promptly upon Public Sector Entity's discovery or knowledge thereof. Bank shall have no responsibility or liability for any errors or inaccuracies contained in any Image File or other data or information received from Public Sector Entity.

(c) Public Sector Entity shall immediately notify Bank if Public Sector Entity revokes enrollment of any Payor, suspends or cancels any Payor or otherwise suspends or terminates any Payor's access to the Service.

5.2 Statement Notification

(a) Public Sector Entity shall be responsible for the accuracy, adequacy and proper data for all notification email data. Bank will send out statement notification emails to the Payor as specified by Public Sector Entity. Bank shall have no responsibility or liability for any errors or inaccuracies continued in any notification related data or information received from Public Sector Entity.

6. Intellectual Property Ownership. These Service Terms do not transfer to Public Sector Entity any ownership, intellectual property or proprietary rights in the Technology or any work or any part thereof, or any copyright, trademark, patent right, etc., and all right, title and interest in and to the Technology and intellectual property will remain solely with Bank or its licensors. Bank hereby grants Public Sector Entity the non-exclusive, non-assignable, non-sub licensable right to display the J.P. Morgan Logo (a) in a form to be provided by Bank, (b) solely on Public Sector Entity's Internet website and (c) solely in connection with Public Sector Entity's use of Bank's Pay Connexion product as described in these Service Terms (the "Permitted Purpose"). Public Sector Entity will use the J.P. Morgan Logo only for the Permitted Purpose and only in accordance with any quality standards and specifications supplied or approved by Bank. Public Sector Entity will, upon Bank's request, (a) submit to Bank for prior approval all proposed uses of the J.P. Morgan Logo and (b) provide to Bank samples of existing uses of the J.P. Morgan Logo and any other documents or information which may permit Bank to determine if Public Sector Entity's use of the J.P. Morgan Logo meets quality standards and specifications and directions supplied or approved by Bank. Ownership of the J.P. Morgan Logo and the goodwill relating thereto shall remain vested in Bank both during the period of these Service Terms and thereafter. Any use of the J.P. Morgan Logo by Public Sector Entity shall inure to the benefit of Bank. Public Sector Entity grants Bank a non-exclusive limited license to use Public Sector Entity's name, trademarks, service marks, symbols, logos, domain names and trade names, as applicable, for use in connection with the provision of Services, upon request and approval of the City.

7. Warranties, Indemnity, Disclaimers and Limitations of Liability.

7.1 Public Sector Entity Warranty and Reimbursement. With respect to ACH transactions processed by Bank for Public Sector Entity pursuant to these Service Terms, Public Sector Entity is deemed to provide to Bank the same warranties to Bank that Bank is deemed to make under the NACHA Rules, and as between Bank and Public Sector Entity, the Bank will have no responsibility with respect to matters so warranted. Public Sector Entity shall not be deemed to warrant, however: (i) the power of Bank under applicable law to comply with the requirements of the NACHA Rules; or (ii) the conformity of debit entries transmitted by Bank to the file specifications contained in the NACHA Rules. Public Sector Entity further represents, warrants and covenants that: (a) Public Sector Entity shall comply with the Rules and Regulations applicable to Public Sector Entity; (b) Public Sector Entity has the authority to enter into these Service Terms and perform its obligations hereunder; and (c) Public Sector Entity will not use or include the full Social Security number of any Payor as a customer identifier or for any other purpose related to the Services. Should Public Sector Entity receive notice of any claim regarding the Services, Public Sector Entity shall promptly provide Bank with a written notice of such claim.

7.2 Bank Warranty. Bank warrants that (i) Bank has the authority to enter into these Service Terms and perform its obligations hereunder; (ii) Bank shall comply with the Rules and Regulations applicable to Bank as provider of the Services; and (iii) the Services will substantially conform to the specifications set forth in the SLA or any SOW, as applicable.

7.3 DISCLAIMER. EXCEPT AS SET FORTH ABOVE IN SECTION 7.2, BANK MAKES NO REPRESENTATIONS OR WARRANTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY REGARDING OR RELATING TO ANY OF THE TECHNOLOGY OR SERVICES AND/OR ACCESS TO OR USE OF THE SERVICES OR TECHNOLOGY PROVIDED TO PUBLIC SECTOR ENTITY HEREUNDER. BANK SPECIFICALLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. BANK ALSO DOES NOT GUARANTEE THAT PUBLIC SECTOR ENTITY'S ACCESS TO THE SERVICES PROVIDED HEREUNDER WILL BE UNINTERRUPTED, ERROR FREE OR SECURE. BANK DOES NOT WARRANT THE ACCURACY, RELIABILITY, COMPLETENESS OR TIMELINESS OF THE CONTENT OF INTERNET WEBSITES OR OTHER DATA RECEIVED BY PUBLIC SECTOR ENTITY OR PAYORS VIA THE INTERNET.

7.4 Limitation of Liability. Bank's liability for any loss or damage arising out of or related to these Service Terms (whether arising out of third party claims, breach of warranty, or otherwise), regardless of the form of action, shall be limited to direct damages resulting from Bank's gross negligence or willful misconduct in providing the Services. Bank shall be entitled to rely on the content, accuracy and completeness of all information and data supplied to Bank by Public Sector Entity. Public Sector entity shall be solely liable for the security and integrity of all information and data supplied or transmitted to Bank including during transmission to Bank.

7.5 Consequential Damages. Except for liability of the parties arising under the NACHA Rules, neither party shall be liable for any special, incidental, indirect, punitive, exemplary or consequential damages whatsoever (including, but not limited to, damages for loss of revenues or profits, for business interruption, or for loss of privacy) arising out of or in any way related to these Service Terms or the use of or inability to use the Services, regardless of the form of action and even if advised of the possibility of such damages. Any fines, fees, penalties or assessments imposed by the Payment Brands related to the provision of Services shall not be deemed to be consequential damages.

8. Term and Termination.

8.1 Term. These Service Terms will be effective commencing on the Service Start Date, and continuing for three (3) years (the "Initial Term"). Following the Initial Term, these Service Terms can be renewed for successive two-year terms (each, a "Renewal Term") unless (a) terminated earlier as set forth below, or (b) either party notifies the other of its desire to terminate the Service Terms at least sixty (60) days prior to the expiration of the Initial Term or the then current Renewal Term.

8.2 Termination. These Service Terms may be terminated as follows:

(a) If Public Sector Entity fails to make any payment due, if applicable, hereunder, and fails to cure such breach within thirty (30) days after receiving written notice from Bank, then Bank may immediately and without further notice, terminate these Service Terms.

(b) Except as set forth in subsection 8.2(a) above, if either party materially breaches any term or condition of these Service Terms and fails to cure such breach within sixty (60) days after receiving written notice of the breach, the non-breaching party may terminate on written notice at any time following the end of such sixty (60) day period.

(c) Either party may terminate these Service Terms upon written notice to the non-terminating party in the event of the non-terminating party's inability to meet its debts as they come due, receivership or voluntary or involuntary bankruptcy or the institution of any proceeding thereof, or any assignment for the benefit of the non-terminating party's creditors, or a determination by the terminating party, in its reasonable discretion, that the financial condition of the non-terminating party has become materially impaired.

(d) Bank may terminate these Service Terms upon not less than one hundred eighty (180) days prior written notice to Public Sector Entity if Bank ceases to provide the Service to its customers generally.

(e) Bank may terminate these Service Terms in the event Bank makes a good faith determination that Public Sector Entity's use of the Service or any portion is in violation of Rules and Regulations, in which case Bank shall terminate these Service Terms immediately, but shall use reasonable diligence to give as much advance notice as feasible, and where commercially feasible under the circumstances, shall give Public Sector Entity a reasonable opportunity to cure prior to any such termination.

8.3 Effect of Termination. Upon termination or expiration of these Service Terms, all rights to the Services and Technology, including, but not limited to use and access, will automatically terminate. Public Sector Entity will discontinue its use of the Services and Technology, and upon request from Bank, will return to Bank any and all Services, equipment, software, documentation, Technology or other deliverables provided to Public Sector Entity by Bank, including any copies thereof held by Public Sector Entity. The provisions of sections 7 and 9 shall survive termination of these Service Terms.

9. Confidentiality.

9.1 Bank Information. Public Sector Entity acknowledges that the Technology and Services contain valuable trade secrets and other nonpublic or proprietary information which is the sole property of the Bank or its licensors ("Bank Confidential Information"), and Public Sector Entity agrees to hold same in confidence and disclose only to those employees or agents whose duties reasonably require access to same. Public Sector Entity will use the same care and discretion to avoid unauthorized use, disclosure, publication, access or dissemination of Bank Confidential Information received from Bank or through the Service as Public Sector Entity uses with its own similar information (but in no event less than a reasonable degree of care).

9.2 Public Sector Entity Information. The Bank acknowledges that Public Sector Entity's systems may contain valuable trade secrets and other nonpublic or proprietary information including information regarding its Payor customers, which are the sole property of Public Sector Entity, and that Bank may maintain, process or otherwise be permitted access to other Payor information through the Service which is of a nonpublic, personal nature (collectively referred to herein as "Public Sector Entity Confidential Information") and the Bank agrees to hold same in confidence. The Bank will use the same care and discretion to avoid unauthorized use, disclosure, publication, access or dissemination of Public Sector Entity Confidential Information received from Public Sector Entity or through the Service as Bank uses with its own similar information (but in no event less than a reasonable degree of care). Bank will use Public Sector Entity Confidential Information only to perform its obligations under these Service Terms. Notwithstanding the foregoing, the Bank may disclose such Public Sector Entity Confidential Information to affiliates, agents and other third parties, including counsel and regulators, and their employees, as reasonably required for Bank to provide the Services or as otherwise required by applicable law or regulation.

9.3 Exceptions. The obligations of this Section 9 shall not apply to any Bank Confidential Information or Public Sector Entity Confidential Information (collectively, "Confidential Information") that: (a) is now, or hereafter becomes, through no act or failure to act on the part of the receiving party (the "Receiver"), generally known or available; (b) is known by the Receiver at the time of receiving such Confidential Information, as evidenced by the Receiver's records; (c) is hereafter furnished to the Receiver by a third party, as a matter of right and without restriction on disclosure; (d) is independently developed by the Receiver without reference to or use of the disclosing party's Confidential Information; or (e) is required to be disclosed by law or in connection with a legal or administrative proceeding, provided that the party to whom the Confidential Information belongs is given prompt prior written notice of such proposed disclosure, provided such notice is not otherwise prohibited, and provided further, that Bank may disclose Confidential Information to any bank regulatory authority having jurisdiction over Bank without notice.

9.4 Data in Aggregate Form The restrictions on use in this Section 9 shall not apply to information or data in aggregated and/or anonymized form, and shall not prohibit the use by Bank of any statistical, aggregate information that is not identified with Public Sector Entity or any Payor for creation of statistical marketing studies for research, product development and promotion, or strategic planning. Further, notwithstanding anything in this Section 9, should Bank have any agreement with a Payor who is also a Bank customer that applies to the use of such Payor's information, the terms of such agreement shall not be affected by the terms of these Service Terms and shall remain in full force and effect.

10 Miscellaneous Provisions.

10.1 Restricted Rights. Technology or Services acquired with United States Federal Government funds or intended for use within or for any United States federal agency are provided with "Restricted Rights" as defined in DFARS 252.227-7013(c)(1)(ii) or FAR 52.227-19.

10.2 Relationship of Parties. The parties are independent contractors. Neither party shall be deemed to be an employee, agent, partner or legal representative of the other, and neither party shall have any right, power or authority to create any obligation or responsibility on behalf of the other except as specified herein.

10.3 Entire Agreement; Amendments. These Service Terms, including the Account Documentation, the Exhibits hereto and all materials and documents referred to herein, sets forth all of the promises, agreements, conditions and understandings between the parties respecting the subject matter hereof and supersedes all negotiations, conversations, discussions, correspondence, memoranda and agreements between the parties concerning the subject matter hereof. In the event of conflict between the Account Documentation and these Service Terms, these Service Terms shall control. Except as otherwise provided, these Service Terms may not be modified except by in writing signed by authorized representatives of both parties.

10.4 Third Party Beneficiaries. The parties intend that these Service Terms shall not benefit or create any right or cause of action in or on behalf of any person or entity other than the parties.

10.5 Notices. All notices required or permitted to be given hereunder shall be addressed as set forth below or as otherwise agreed in writing by the parties from time to time.

10.6 Severability. If any provision in this Agreement is held to be inoperative, unenforceable, or invalid, such provision shall be inoperative, unenforceable, or invalid without affecting the remaining provisions, and to this end the provisions of this Agreement are declared to be severable. Failure of either party to exercise any of its rights in a particular instance shall not be construed as a waiver of those rights or any other rights for any purpose.

10.7 Force Majeure. Bank and City shall not be held responsible for any act, failure, event or circumstance addressed herein if such act, failure, event or circumstance is caused by conditions beyond its reasonable control.

10.8 Governing Law. THIS AGREEMENT AND ANY CLAIM, CONTROVERSY OR DISPUTE ARISING UNDER OR RELATED TO THIS AGREEMENT, THE RELATIONSHIP OF THE PARTIES, AND/OR THE INTERPRETATION AND ENFORCEMENT OF THE RIGHTS AND DUTIES OF THE PARTIES SHALL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF TEXAS, WITHOUT REGARD TO ANY CONFLICTS OF LAW PRINCIPLES, BUT GIVING EFFECT TO FEDERAL LAWS APPLICABLE TO NATIONAL BANKS. CLIENT HEREBY WAIVES ANY RIGHT TO PERSONAL SERVICE OF ANY PROCESS IN CONNECTION WITH ANY ACTION, AND HEREBY AGREES THAT SERVICE MAY BE MADE BY REGISTERED OR CERTIFIED MAIL.

Effective as of the _____ day of _____, 20__.

	CITY OF AUSTIN		JPMORGAN CHASE BANK, N.A.
By:	Teresa Reddy	By:	Larnell Camus
Name:	Teresa Reddy	Name:	Larnell Camus
Title:	Corp Contract Compliance Manager	Title:	Senior Banker
Address for Notices:	124 W. 8th Street, Ste. 310		300 S. Riverside Plaza, Suite IL1-0199
	Austin, TX 78701		Chicago, Illinois 60606
			Attn: Pay Connexion
Phone/ Fax:	512.974.1421 /	Phone/ Fax:	312.954.3545 / 312.954.3516

Public Sector Entity Attestation:

The undersigned, a duly authorized officer or representative of the Public Sector Entity, does hereby certify that the Public Sector Entity has been duly authorized to enter into and perform this Agreement and that the person signing above on behalf of the Public Sector Entity,

whose execution of this Agreement was witnessed by the undersigned, is an officer, partner, member or other representative of the Public Sector Entity possessing authority to execute this Agreement.

By: _____*

Name: DAVID KUCKO

Title: Corporate Contract Administrator

*Note: The person signing the attestation shall be someone different from the person signing above on behalf of the Public Sector Entity.

Exhibit C
Pay Connexion Standard Service Level Agreement

PAY CONNEXION℠ STANDARD SERVICE LEVEL AGREEMENT

I. OVERVIEW

This Service Level Agreement (SLA) has been created to formalize agreed upon levels of service with respect to the development efforts and Services provided by Bank to Public Sector Entity in accordance with the Pay Connexion℠ Service Terms. The service level standards will incorporate measurable criteria in order that performance can be monitored on an ongoing basis. The agreement to these standards affirms the commitment of both organizations to establish and maintain quality service levels. Notwithstanding anything to the contrary herein or in the service terms, the SLA establishes target levels only and failure to achieve any target level will not be deemed to be a failure by Bank to exercise ordinary care.

II. PRODUCT & SERVICE OFFERING

o DEFINITIONS

Unless as otherwise defined below, capitalized terms found in this document shall have the meanings defined in the Pay Connexion℠ Service Terms.

Term	Meaning
Dark Window	The time period when Scheduled Maintenance (defined below) may be conducted by Bank on the Services. For the purposes of this document, the Dark Window is scheduled to occur on Saturdays and Sundays from 01:00 AM to 07:00AM Eastern Time(ET), unless Bank notifies Public Sector Entity of a change to the Dark Window schedule.
Scheduled Maintenance	Maintenance on the Services that occurs during the Dark Window or other agreed upon period of time.
System Outage	The time period when the ability to accept and process payments is unavailable for use by Public Sector Entity or Payors, other than in a Dark Window.
Uptime	The number of minutes that the application is available to receive and process payments
Change Management Process	The process used to document and implement changes to a production application. Each request will be managed according to defined timelines and the existing queue of development efforts.
Production Support	The JPMC functional team that manages issue resolutions in accordance with the service levels stated herein. This team also manages all change requests and operations monitoring.

o PRODUCT AND SERVICE OFFERING

The Services to be provided by Bank have been designed and developed to meet Public Sector Entity's payment collection needs for consumer Payors. Public Sector Entity acknowledges the Services offered by Bank will be hosted in a shared services infrastructure.

o ENROLLMENT

If required by the configuration of Services chosen, Public Sector Entity agrees to provide to Bank a current and complete electronic file of Public Sector Entity information in a format mutually acceptable to Bank and Public Sector Entity to facilitate the initial database import of Public Sector Entity Payor information into the Pay Connexion Transaction System (the "Pre-Registration File"). Public Sector Entity agrees to provide Bank the Pre-Registration File no later than seven (7) Business Days prior to the Pay Connexion Transaction System production launch date.

Thereafter, Public Sector Entity agrees to provide Bank a daily file in the same format that contains any associated changes, additions, or deletions that are relevant to the Pay Connexion Transaction System. Public Sector Entity agrees to provide Bank the Pre-Registration File each night by no later than 9:00PM Eastern Time (ET) after the initial provision of the Pre-Registration File.

- **PERFORMANCE STANDARDS AND EXCEPTIONS**

(Applicability is dependant on the configuration of the services chosen by Public Sector Entity)

Technology Service Level Description	Minimum Service Level Criteria
Web Availability / Uptime	Goal: Pay Connexion℠ Transaction System web applications will be available to users ninety-nine percent (99%) of the total minutes available in each month. Availability is calculated excluding any Scheduled Maintenance or scheduled System Outages. In addition, there shall be no more than two (2) System Outages (planned or unplanned) during each twenty-four (24) hour period (measured from midnight to midnight), and the aggregate time of the System Outages during that period shall not exceed two (2) hours.
IVR Availability / Uptime	Goal: Pay Connexion Transaction System IVR applications will be available to users ninety-nine percent (99%) of the total minutes available in each month. Availability is calculated excluding any Scheduled Maintenance or scheduled System Outages. In addition, there shall be no more than two (2) System Outages during each twenty-four (24) hour period (measured from midnight to midnight), and the aggregate time of the System Outages during that period shall not exceed two (2) hours.
Web and IVR Disaster Recovery	Provide an offsite hot backup site. Primary processing capabilities will be available within 8 hours if primary site is disabled.
Web and IVR Backup Recovery Testing	The backup recovery systems to be tested annually.
Standard Pre-Registration File Processing	Billers with the Pre-Registration feature are required to deliver a Pre-registration file to the Pay Connexion team by 9pm Eastern time in accordance with their daily delivery schedule. Pay Connexion will process the Pre-registration file upon receipt from the biller or an intermediary. Response files will be delivered to the biller by 9AM Eastern time, in accordance with the Biller's daily delivery schedule. If the Biller does not deliver a Pre-registration file on time the Pay Connexion team will make best efforts to meet the 9AM delivery Response file but will not guarantee a 9AM delivery time.
Standard Next Day Remittance File Processing	The Pay Connexion team will deliver a Remittance file to the Biller (either directly or through an intermediary) by an agreed upon time, Monday through Friday, excluding Federal Reserve holidays.
Standard Same Day Remittance File Processing	The Pay Connexion team will deliver a Remittance file to the Biller (either directly or through an intermediary) by an agreed upon time, Monday through Friday, excluding Federal Reserve holidays.

Call Center Service Level Description	Minimum Service Level Criteria (based on a minimum of 500 calls per month)
Call Center Availability	Standard hour of operations are 24 x 7 x 365
Languages supported by the call center	English and Spanish (live operator)
Monitored calls answered accurately	To monitor how Public Sector Entity Service Agents handle inquiries. Operators will be measured on the accuracy of the information they provide, their interpersonal manner, and whether they follow the scripts. MAP goal shall be 95% of all monitored calls to be answered accurately. Monitoring shall occur on a minimum of 3 calls per agent per week.
Incoming Calls Lost	To monitor queue size for Public Sector Entity Service. This information is received from the telephone switch, and will be measured at the Automated Call Distribution (ACD) level.

	MAP goal for incoming calls lost due to forced busy and forced disconnects (i.e. not enough capacity) shall be that such calls do not exceed 3% of all calls received
Percent Abandoned Incoming Calls	To monitor the number of calls which are abandoned after being put in the queue. The calls will be measured beginning when they are put in the queue to the point when the caller hangs up. MAP goal for the percentage of calls queued to live agents that do not get answered shall be that such calls do not exceed 6% of the total number of calls received.
Calls Answered in 30 Seconds or Less By Operator	To monitor the speed with which calls are answered in aggregate. The calls will be measured beginning when they enter the agent queue to the point when the call is answered. This information is received from the telephone switch, and will be measured at the ACD level. MAP goal for calls answered in 30 seconds or less shall be that at least 70% of all incoming calls queued to live agents be answered in 30 seconds or less.
Call Center Disaster Recovery	Provide an offsite hot backup site. Primary call center functions will be available within 16 hours if primary site is disabled.
Call Center Backup Recovery Testing	The backup recovery systems to be tested at least annually.

III. OUTAGE NOTIFICATION

A. PLANNED / SCHEDULED OUTAGES

In the event of any planned or scheduled System Outages, it is expected that Bank will contact the appropriate individuals designated by Public Sector Entity at least twenty-four (24) hours prior to the planned System Outage (contact information will be amended from time to time via e-mail). Additionally, in the event of a planned / scheduled System Outage, it is expected that Bank will adhere to the following guidelines:

1. Downtime will be scheduled during standard maintenance windows of Saturday and Sunday 01:00 AM –07:00 AM Eastern Time (ET), except as necessary and upon notice as provided above.

2. Bank will implement a web page on the payer site notifying that the system is unavailable during the scheduled downtime (Bank will immediately remove this notification page following completion of the scheduled maintenance).

3. Bank will implement a message on the IVR notifying that the system is unavailable during the scheduled downtime. (Bank will immediately remove this message following completion of the scheduled maintenance).

B. UNPLANNED / UNSCHEDULED OUTAGES

Bank will adhere to the Severity Level requirements for unscheduled System Outages/service interruptions according to the table in this Section III B. Unless otherwise specified, all hours referred to in this Section III B are clock hours.

Severity Level / Response Time SLA

Severity Level Definition	Initial Contact w/ Clients / Internal Functional Teams	Resolution Goal
Primary Definition: ▪ Severity 1 (Emergency) Degeneration in or complete failure of, the system or a any single channel (IVR, Web, Admin) to receive and process payments. ▪ Restricted to true, system-wide emergencies. A complete failure has occurred in either a system or critical process.	15 min to Client contacts and/or Internal Functional Team Designate (TBD); hourly updates until resolved	ASAP – no later than end of Business Day

Severity Level Definition	Initial Contact w/ Clients / Internal Functional Teams	Resolution Goal
Primary Definition: • Severity 2 (High) Degeneration in, or complete failure of, business-critical secondary functionality (RTPC, all file processing, password reset, download a Remittance File, or the ability to initiate a call) for a single Biller or group of Billers • Used when the problem is severely affecting a group of users. A major portion of a system or process is not functional, but can be bypassed, or it is a functional failure with no workaround.	15 min to Client contacts and/or Internal Functional Team designate (TBD); hourly updates until resolved	ASAP – no later than end of 2nd Business Day
Primary Definition: • Severity 3 (Medium) Degeneration in product functionality of non-critical tertiary functionality (confirmation emails, standard reporting, etc) for a single Biller or a group of Billers • This is the most common severity level. A system or process is mostly functional but not performing as expected. An error can be ignored, or a workaround can be used.	Monthly issues log	As prioritized in release by Product Management.
Primary Definition: • Severity 4 (Low) System or critical process is functional, but a problem exists related to ease of use (slow app response time or screen flows), interface or Standard Report content, or a problem exists for a single payer or group of Payers (can't reset passwords, can't log in). • A single Payer is impacted. A system or process is currently fully functional but a problem exists, or the problem relates to information, process change(s), minor enhancement(s), or request(s) for future functionality.	Monthly issues log	As prioritized in release by Product Management.

IV. GENERAL SUPPORT EXPECTATIONS

A. SUPPORT

Tier I Support Telephone-based support whereby Public Sector Entity's Payors access a Public Sector Entity support representative for assistance on Payor-related issues specific to the Services during regularly scheduled Payor service hours.

Tier II Support Telephone-based support whereby Public Sector Entity's support representative can call a Bank support representative for assistance on Payor-related issues specific to the Services.

Tier III Support Telephone-based customer support whereby Bank support representatives escalate Service problems to internal technical resources for issue resolution.

Bank will only provide Tier I support in cases where Public Sector Entity requests assistance as part of the IVR channel service (roll-out operator support). Tier II customer service representatives resolve those calls for which Tier I staff require assistance. Tier II requests may require additional internal/external investigation to be performed by dedicated staff. Tier III support representatives will be responsible for analysis and resolution of technical or other system-related problems. Tier III support will be staffed and supported by Bank technical or knowledge subject matter experts. Public Sector Entity will be able to contact the following toll-free number for Tier II support, technical issues, or to report system interruptions: 886-282-1981.

B. PRODUCTION EXPECTATIONS

When Public Sector Entity's Pay Connexion system is in production, Bank will be responsible for the following in addition to the service levels identified herein:

- Housing the system in a secure environment and adherence to regulatory and audit requirements of this kind of payment system. Security is defined as utilizing proper encryption and access control standards.
- If using Bank Call Center, authentication of users as they enter the system pursuant to Bank policies and procedures.
- Archival of pre-registration file for 2 weeks after acceptance for possible retrieval.

- Initiation of the RTPC and API transaction in the appropriate format in a timely manner. (Optional Service)
- Processing payments through the appropriate payment channels as configured during set up.
- Making data available for reporting queries initiated through the Pay Connexion Administrative system for two years standard
- Send emails as indicated in the Functional Specification to either internal resources or to the Payer directly based on events in the payment process.
- Pre-Registration File Processing as described in the SLA herein
- Next Day Remittance Processing as described in the SLA herein
- Same-Day Processing Remittance Processing as described in the SLA herein

When Public Sector Entity's Pay Connexion system is in production, Public Sector Entity will be responsible for the following:

- Providing daily updates to the Pre-Registration file (if selected) for retrieval by Bank by 9:00PM ET.
- Retrieve the remittance file delivered each Business Day by Bank
- Ensure that all data required in the session transfer, as part of the Pre-Registration file or API, is made available as appropriate for processing payments. If a data element is missing or is sent in plan text when it is expected to be encrypted the session will error for the Payer.
- Notify JPMC in advance of infrastructure changes that may impact session transfer, email confirmations, FTP transmissions, and successful RTPC receipt.

V. PROGRESSIVE CONTRACT ADMINISTRATION

It is Bank's intent to work in partnership with Public Sector Entity to resolve all quality issues. Public Sector Entity will be given a written notification of breach of a service level.

Bank will not be deemed to be in material breach (including without limitation a missed cut-off time or delivery schedule) of this SLA if equipment owned by or the responsibility of Public Sector Entity, its affiliates, or any of Public Sector Entity's third party vendors, or the actions or inaction of Public Sector Entity, its affiliates, or any of Public Sector Entity's third party vendors, is determined to be the cause of such breach; or if such breach is the result of circumstances beyond the reasonable control of Bank, provided Bank has exercised such diligence as the circumstances require.

VI. CHANGE MANAGEMENT

A. PRODUCTION CHANGES

Any changes to a production application requested by Public Sector Entity will follow the Change Management process as part of the Production Support function offered by JPMC. Requests for standard features available in the application will be delivered without additional charge for the first 60 days following the launch of an application. After 60 days, Public Sector Entity can request standard features that do not exceed 40 hours of development/testing in each calendar year. All development beyond 40 hours will be charged at the then current hourly rate. All requests for non-standard changes to a production application will be charged at the then current hourly rate.

B. CHANGES DURING IMPLEMENTATION

While the application is in implementation, the client can change any standard feature covered in the original agreement. Any non-standard changes will be charged at the then current hourly rate.

VII. REVIEWS AND MEETINGS

AD HOC REVIEWS

The Parties agree to participate in periodic project and production meetings using any mutually acceptable means of communication. The Parties agree to provide at least seven (7) Business Days notice when requesting an Ad Hoc review. These reviews will include the following elements:

- Review the Issues Log, service levels, cost savings opportunities, industry best practices, and short and long-term milestones.
- Facilitate a frank discussion of key mutual objectives and assess the Parties' progress towards those objectives.

Exhibit DI FEE SCHEDULE

Option A: City-Funded (Charged to Public Sector Entity via Account Analysis)

Implementation Fees:

- Web initiated payments (per web biller) - $1,000
- IVR initiated payments (per IVR biller) - $2,500
- Web & IVR (per web and IVR biller) - $3,000

Monthly Hosting Fees:

- Web initiated payments (per web biller) - $150 per month[1]
- IVR initiated Payments (per IVR biller) - $1 per month[1]
- Web & IVR (per web and IVR biller) Initiated Payments (first IVR biller) - $300 per month[1]

Transaction Fees

One-Time Payments	Measurement	Price
Credit/debit card/ACH/eCheck	Per Confirmation Number Generated[2]	$ 0.30

- IVR Call Charge (Telecom) - $.13 per minute
- JPMorgan Chase CSR Support - $1.25 per minute

Statement Image Presentment Fees

- $.20 per image

Notes

[1]Monthly hosting fees include all the maintenance and upkeep of the hosted infrastructure, the daily transmission of remittance files to Customer and the daily delivery of files to process and settle payments via ACH and the Merchant Processor.

[2]The cost of processing and settlement of ACH transactions will apply. If credit cards are to be accepted, the processing and settlement of credit card transactions will be based on arrangements with the Merchant Processor. These fees do not include merchant processing fees for credit card transactions.

Option B: Convenience Fees (Paid by Payer to J.P. Morgan at No Cost to City of Austin)

- **Credit and Debit Card Convenience Fee Payments** (for all convenience fee-funded applications):
  - **Option B1 - Percentage-based convenience fee for MasterCard and Discover Credit and Debit Card Payments**: 2.4% of Payment Amount

  or

  - **Option B2 - Set convenience fee for Visa, MasterCard and Discover Credit and Debit Card Payments:** The convenience fee is based on the average principal payment amount for each application (i.e., Pay Connexion "biller"). The convenience fee is a fixed, flat amount per Credit or Debit Card payment transaction based on the below average principal payment amount tiers. If the average principal payment amount changes for two consecutive months so that the average principal payment amount tier changes, a new convenience fee may be applied based upon the above tiers. When a convenience fee changes, J.P. Morgan will provide at least 30 days written notice.

Average Principal Payment Range	Convenience Fee
$0.01 to $49.99	$1.50
$50 to $99.99	$2.50
$100 to $149.99	$3.50
$150 to $199.99	$4.75
$200 to $299.99	$7.50
$300 to $399.99	$10.00
$400 to $499.99	$12.00
$500 to $599.99	$15.00
$600 to $699.99	$18.00
$700 to $799.99	$21.00
$800 to $899.99	$23.00
$900 to $999.99	$26.00
$1,000 to $1,249.99	$31.00
$1,250 to $1,499.99	$37.00
$1,500 to $1,749.99	$43.00
$1,750 to $1,999.99	$49.00
$2,000 to $2,499.99	$61.00
$2,500 to $2,999.99	$73.00
$3,000 to $3,499.99	$85.00
$3,500 to $3,999.99	$97.00
$4000 to $4499.99	$110.00
$4500 to $4999.99	$122.00
Additional average principal payment ranges can be provided if average principal payment amounts are expected to exceed $4999.99	

- ACH/e-check Payments - $1.00 per Payment Amount

Notes

1. In the event that Public Sector Entity seeks to utilize Pay Connexion to collect any tax payment(s) types, an appropriate alternative tax-specific convenience fee structure will be provided.

2. The selection of either Convenience Fee model Option B1 or Option B2 shall apply to all Convenience Fee-funded applications.

3. Bank must comply with Card Association/Network rules and guidelines. Bank will work with Public Sector Entity to develop and maintain a convenience fee program in accordance with the Associations/Networks.

4. Convenience fees are funded by the Payor and collected directly and automatically by Bank. Although interchange expenses for the processing and settlement of credit/debit card transactions will be charged to Bank by the merchant processor, Chase Paymentech Solutions, LLC. The necessary merchant account(s) for processing of the principal payments must be established. Public Sector Entity will not bear interchange expenses for these transactions.

5. This fee schedule may need to be revised if Public Sector Entity chooses to expand its use of Pay Connexion beyond the scope of the listed applications, or if doing so is required by Card Associations or NACHA.

6. The costs of ACH/e-Check processing and settlement (i.e., fees per ACH item originated or returned) are beyond the scope of this fee schedule.

7. Bank reserves the right to modify pricing upon 30 days written notice in the event Public Sector Entity or Bank become aware of any changes in applicable rules, laws, regulations or case law that would have a negative impact on the manner in which fees are charged hereunder. If either party becomes aware of same, it shall promptly notify the other in writing.

Exhibit E

PAYCONNEXION TRANSACTION ADDENDUM TO SELECT MERCHANT PAYMENT CARD PROCESSING AGREEMENT

MERCHANT NAME: City of Austin
SUBMITTER NAME: JPMorgan Chase Bank, N.A. (PayConnexion)

This PAYCONNEXION TRANSACTION Addendum shall, upon full execution by all parties hereto, modify (i) that certain Contract for Credit Card Processing Services, which includes the State of Texas Chase Paymentech Select Government Merchant Payment Instrument Processing Agreement (inclusively the "Merchant Agreement") between **Paymentech, LLC** ("Paymentech", "we", "our" or "us"), for itself and on behalf of Member and the **City of Austin** (hereinafter referred to as the "Merchant") dated on or about October 6, 2010, and (ii) that certain Select Merchant Payment Card Processing Submitter Agreement (the "Submitter Agreement") between Paymentech and JPMorgan Chase Bank, N.A. (as successor in interest to Bank One, N.A.; hereinafter referred to as the "Submitter") dated as of May 5, 2004.

WHEREAS, Merchant has entered into the "Pay Connexion Service Terms with Submitter for the provision of Pay Connexion services;

WHEREAS, pursuant to the Pay Connexion Service Terms, Submitter will capture Transaction Data from Merchant's Customers on behalf of Merchant and submit such Transaction Data to Paymentech for processing ("Payconnexion Transactions");

WHEREAS, if applicable, Merchant may also accept Payment Instruments from Customers directly, which will be submitted directly to Paymentech from Merchant pursuant to the terms of the Merchant Agreement;

WHEREAS, Paymentech desires to process all Transactions submitted to Paymentech (whether directly by Merchant or through Submitter, as applicable);

1. **APPLICABILITY OF MERCHANT AGREEMENT.** Unless otherwise indicated in this Addendum, capitalized terms in this Addendum have the meanings set forth in the Merchant Agreement. The terms and conditions of this Addendum apply to all PAYCONNEXION TRANSACTIONS processed pursuant to this Addendum. **Unless expressly contradicted by this Addendum, all terms of the Merchant Agreement and the Submitter Agreement shall apply to the processing of PAYCONNEXION TRANSACTIONS.**

2. **DEFINITIONS.**

   CONVENIENCE FEE TRANSACTION DATA is the evidence and electronic record of a transaction representing a charge to a consumer's Card or checking account for the convenience of using the payment channel offered by the Merchant and Submitter.

   PAYCONNEXION TRANSACTION is a transaction submitted to Merchant by a Cardholder over IVR, the World Wide Web, or other card not present forum, which Merchant submits to Submitter, and which Submitter in turn submits to Paymentech for processing. PAYCONNEXION TRANSACTIONS may be comprised of both a CONVENIENCE FEE TRANSACTION and Transaction Data.

3. **PROCESSING AND PAYMENT.**

   a. Merchant and Submitter hereby agree that, with respect to all PAYCONNEXION TRANSACTIONS, (i) all CONVENIENCE FEE TRANSACTION DATA will be submitted by Submitter to Paymentech under the Submitter Agreement, (ii) all Sales Data will be submitted by Submitter on behalf of Merchant to Paymentech under the Merchant Agreement, (iii) if the PAYCONNEXION TRANSACTION includes both CONVENIENCE FEE TRANSACTION DATA and Sales Data, all Paymentech processing fees, chargeback fees, funds transfer fees, interchange and assessment fees, or other fees that may apply associated with CONVENIENCE FEE TRANSACTION DATA and Sales Data shall be paid by Submitter pursuant to the terms of the Submitter Agreement, (iv) if the PAYCONNEXOIN TRANSACTION includes both CONVENIENCE FEE TRANSACTION DATA and Sales Data, all chargebacks, returns and similar charges related to Sales Data shall be paid by Merchant pursuant to the terms of the Merchant Agreement, (vi) if the PAYCONNEXION TRANSACTION includes only Sales Data, all Paymentech processing fees, chargeback fees, fund transfer fees, interchange and assessment fees, or other fees that may apply associated with processing Sales Data shall be paid by the Merchant pursuant to the terms of the Merchant Agreement. (vii) if the PAYCONNEXION TRANSACTION includes only Sales Data, all chargebacks, returns and similar charges related to Sales Data shall be paid by Merchant pursuant to the terms of the Merchant Agreement, (viii)settlement funding for CONVENIENCE FEE TRANSACTION DATA will be paid directly to a bank account designated by Submitter, (ix) settlement funding for Sales Data will be paid directly to a bank account designated by Merchant, and (x) all information related to Sales Data, chargebacks, returns, settlement funding and other information provided to Paymentech pursuant to the Merchant Agreement may be disclosed by Paymentech to the Submitter.

4. **FEES.**

Unless the Pay Connexion Service Terms specifically state otherwise, Merchant is directly responsible for paying the processing fees set forth on Schedule A to the Merchant Agreement. Specifically, this Section 4 and Schedule A shall not apply if the Pay Connexion Service Terms state that Service Provider is responsible for paying Merchant Processor's processing fees and other similar fees and charges.

Your signature on two copies of this Addendum that you return to us indicates your understanding and acceptance of its terms and incorporation by reference in the Merchant Agreement and the Submitter Agreement.

[Signature Page Follows]

Agreed and Accepted by:

City of Austin

MERCHANT LEGAL NAME (Print or Type)

Address (Print or Type)

By (authorized signature)

Teresa Reddy Core Contract Compliance Manager

By, Name, Title (Print or Type)

3/20/13

Date

Agreed and Accepted by:

JPMorgan Chase Bank, N.A.

SUBMITTER LEGAL NAME (Print or Type)

By (authorized signature)

Larnell Camus, Senior Banker

By, Name, Title (Print or Type)

March 12, 2013

Date

PAYMENTECH, LLC for itself and on behalf of Member

By:

Print Name: Bob Young

Title: Director - Credit

Date: 3/12/13

Address: DALLAS, TX

Exhibit F

Chase Onsite Card Payments

Annual Onsite Card Payments Convenience Fee Compliance Attestation

J.P. Morgan Chase Bank, N.A., operates its Pay Connexion and Onsite Card Payment programs which may include processing point-of-sale payments with convenience fees. As you were instructed during the implementation of these programs, the Federal Reserve Bank, Card Brands (Visa, MasterCard and Discover) have rules about the manner in which convenience fees can be collected. These rules and regulations may change from time-to-time. The signed Service Terms indicate that you comply with these federal regulations and Card Brand rules.

It is important that J.P.Morgan Chase Bank, N.A. ask for your compliance confirmation in these important Card Brand Rules:

1. **Charging Convenience Fees** – If you are collecting convenience fees at the point-of-sale or through Pay Connexion's Web Site or phone channels, you must not charge additional convenience fees or surcharges (other than the single convenience fee that J.P. Morgan charges).
2. **Disclosures Relating to Convenience Fees** - If you are collecting convenience fees at **the point-of-sale**, you must adequately post required disclosures relating to the collection of the convenience fees.

   Required convenience fee disclosures:
   1. Post signage prominently at the point-of-sale with the details of the convenience fee

   Other best practices about convenience fee disclosures include:
   2. Post the details of the convenience fee on your web site and other areas where you communicate details about payment collection
   3. Verbally communicate to cardholders that convenience fees apply and the details of the convenience fee
   4. Process a Fee Inquiry on the point-of-sale terminal and provide the printout of the transaction detail to the cardholder

J.P. Morgan Chase Bank, N.A. performs an annual audit of its clients using convenience fee programs. We request our clients confirm their compliance with Card Brand requirements specific to method of payment acceptance and disclosures relating to convenience fees.

I, hereby attest that the below entity is following proper Card Brand method of payment acceptance, as described above. I confirm that if the entity is collecting a payment type other than taxes, it is not accepting Visa as a method of payment.

I, hereby confirm the below entity is following proper Federal Regulations and Card Brand convenience fee disclosures, as described above. Minimally, proper disclosures include posting signage at the point-of sale with the following details:

1. The specific convenience fee pricing
2. The ability for the cardholder to request and approve the specific convenience fee amount prior to payment completion
3. The convenience fee amount will be listed on the payment receipt

A sample of the proper signage is indicated below. You will be provided with the specific signage that you must adequately post.

For your convenience Public Sector Entity accepts credit/debit cards.

- Our service provider will charge a convenience fee that will be added to your payment amount for each transaction.
  - #.#% will be added to your payment amount.
  - There is a minimum charge of $#.##.
- Before you pay, upon request, we can provide you the total of the payment amount, including the convenience fee.
- If you do not wish to pay a convenience fee, do not complete the transaction using a credit or debit card.
- The amount of the convenience fee will be listed on your receipt.

VISA MasterCard DISCOVER NETWORK

The products and services above are offered by JPMorgan Chase Bank, N.A. member FDIC, or its affiliates. © 2012 JPMorgan Chase & Co. All rights reserved.

Sample

Name of Entity

Signature Date

Print Name

Address, City, State, Zip Code