CS-15-98

CONTRACT APPROVAL FORM

(Contract Management Use only)

CONTRACT TRACKING NO.

CM2272-A1

CONTRACTOR INFORMATION

Name: Bill2Pay

Address: 4700 140th Avenue N., Suite 106 Clearwater, FL 33762-3846
(City, State, Zip)

Contractor's Administrator Name: Iris Kraft Title: Co-President/Chief Operations Officer

Tel#: 727-449-3940 Cell: 727-902-5406 Email: iris.kraft@bill2pay.com

CONTRACT INFORMATION

Contract Name: Payment processing Services Agreement Contract Value: N/A

Brief Description: Execution of a PCI Responsibility Matrix and Agreement

Contract Dates : From: _____ to _____ Status: ___ New _X_ Renew _ Amend# ___ WA/Task Order

How Procured: __ Sole Source ___ Single Source ___ ITB ___ RFP ___ RFQ ___ Coop. _X_ Other Financial Service

If Processing an Amendment:

Contract #: CM2272 Increase Amount of Existing Contract: no change in contract terms or dates

New Contract Dates: _____ to _____ TOTAL OR AMENDMENT AMOUNT: _____

APPROVALS PURSUANT TO NASSAU COUNTY PURCHASING POLICY, SECTION 6

1. _____ Department Head Signature _____ Date — Various Departments Funding Source/Acct #

2. Charlotte Young 12/11/15
Contract Management Date

3. _____ 12-14-15
Office of Management & Budget Date
5/12/9/15

4. _____ 12-15-15
County Attorney (approved as to form only) Date

Comments: _____

COUNTY MANAGER – FINAL SIGNATURE APPROVAL

Ted Selby _____ 12/15/15
Date

RETURN ORIGINAL(S) TO CONTRACT MANAGEMENT FOR DISTRIBUTION AS FOLLOWS:

Original: Clerk's Services; Contractor (original or certified copy)
Copy: Department
Office of Management & Budget
Contract Management
Clerk Finance

Bill2Pay

PCI Responsibility Matrix and Agreement

PCI Requirement	Bill2Pay, LLC (Service Provider) Responsibility	Client Responsibility
1: Install and maintain a firewall configuration to protect cardholder data	Limiting network access to and from devices used within the Bill2Pay, LLC online ordering platform to the most restrictive possible	Although not directly handling cardholder data, where applicable client is advised as best practices to maintain firewall configurations that protect internal networks and any data.
2: Do not use vendor-supplied defaults for system passwords and other security parameters	Adhering to CIS-derived system hardening policies for all devices and systems within the Bill2Pay, LLC online ordering platform.	Although not directly handling cardholder data, where applicable client is advised as best practices to not use vendor-supplied defaults or system passwords and other security parameters.
3: Protect stored cardholder data	Securely storing (or not storing) cardholder data within the Bill2Pay, LLC platform in line with PCI Requirement 3.	Not applicable, client does not store cardholder data.
4: Encrypt transmission of cardholder data across open, public networks	Requiring secure transmission of cardholder data into the Bill2Pay, LLC platform and sending data to payment gateways in the most secure manner supported.	Although not directly handling cardholder data, where applicable client is advised as best practices to encrypt transmission of data regardless of type but especially sensitive data.
5: Protect all systems against malware and regularly update anti-virus software or programs	Regularly scanning Bill2Pay, LLC platform servers for malware and viruses with up-to-date anti-virus software.	Although not directly handling cardholder data, client is advised as best practices to protect all systems against malware and regularly update/maintain anti-virus software or programs.
6: Develop and maintain secure systems and applications	Following secure development and change control procedures for all changes to Bill2pay, LLC platform components and ensuring that all Bill2Pay, LLC platform components have the latest	Although not directly handling cardholder data, where applicable client is advised as best practices to follow secure development, change control and patching processes.

	vendor-supplied security patches installed.	
7: Restrict access to cardholder data by business need to know	Restricting access to cardholder data to systems and parties authorized within Bill2Pay, partners or by client.	Not applicable.
8: Identify and authenticate access to system components	Identifying and authenticating access to Bill2Pay, LLC controlled components in PCI scope.	Although not directly handling cardholder data, where applicable client is advised as best practices to identify and authenticate system components but especially sensitive data areas.
9: Restrict physical access to cardholder data	Restricting physical access to Bill2Pay, LLC's platform to PCI level 1 hosting providers.	Not applicable.
10: Track and monitor all access to network resources and cardholder data	Logging and monitoring all activity occurring within the Bill2Pay, LLC Platform	Although not directly handling cardholder data, where applicable client is advised as best practices to track and monitor access to local network resources especially in areas where card scan devices may be installed.
11: Regularly test security systems and processes.	Testing the security systems and processes for the Bill2Pay LLC card processing Platform.	Not applicable.
12: Maintain a policy that addresses information security for all personnel	Maintaining security policies for all Bill2Pay, LLC employees and contractors	Although not directly handling cardholder data, where applicable client is advised as best practices to establish an information security policy for all personnel.

Examples of Bill2Pay's Responsibilities

- Preventing credit card data from being intercepted in-transit between a client submitting credit card data and our platform servers.
- Preventing credit card data stored or transmitted within our platform from being stolen by unauthorized parties.
- Restricting access to sensitive data transmitted and stored by Bill2Pay's platform to only those with a business need.

Bill2Pay

Examples of Client Responsibilities

- Maintaining patched and updated malware tools supporting systems.
- Regularly updating operating systems and applications installed
- Security of third party developers or agencies that develop for client and may interface with Bill2Pay's platforms
- Security of POS system(s) scanners and local environments that interface with Bill2Pay's platforms.

Examples of End-User Responsibilities

- Security of the device or browser being used to enter credit card data. For example, Bill2Pay is not responsible for malicious browser plugins or key loggers.

By this written agreement, known as the "PCI Responsibility Matrix and Agreement", Bill2Pay provides acknowledgement that Bill2Pay, the service provider, is responsible for the security of cardholder data it may possess or otherwise store, process or transmit on behalf of the Client, or to the extent that they could impact the security of the Client's cardholder data. The Client acknowledges and agrees to Bill2Pay's and its responsibilities in the above responsibility matrix.

Bill2Pay LLC

Iris Kraft

Signature

Iris Kraft
Printed Name

Co – President, COO
Title

October 27th, 2015
Date

Nassau County Board of County Commissioners

Signature

T. J. Selby
Printed Name

Co. Mgr
Title

12/15/15
Date