NATPAY

Technical White Paper

This technical white paper discusses:

- *Business Continuity Co-Location*
- *Network Architecture & Security*
- *Database/File Storage Architecture*
- *Scalability*
- *Identify Theft & Data Storage*

About Us

Since its inception in 1991, National Payment (NatPay) has become a leading financial services and information distribution company. We specialize in providing simple, secure, cost-efficient ways for organizations to go paperless via our suite of integrated online products. Our services offer your customers and employees state-of-the-art, self-serve solutions that include direct deposit payroll distribution, payroll pay cards, EZStub electronic pay stubs, and Doculivery™ online documents solutions for customized deployment of statements, W-2s, 1099s, bills with click-to-pay, forms, reports, and a whole lot more!

NatPay and its Doculivery™ Online Document Management Services are SSAE 16 (SOC 1) Type 2 examined, and PCI compliant (level 1). Please see the INDEPENDENT SERVICE AUDITOR'S REPORT at the end of this document for further information.

Business Continuity Co-Location

NatPay has partnered with Peak 10, the Southeast's leading data center operator and managed services provider, to duplicate its production environment in an emergency co-location. Peak 10's facility houses all of our privately owned and operated production equipment.
The following information lists the specifications regarding our hardened computer facility:

SSAE 16 Audits: *Peak 10 is a SSAE 16 examined company.*

Location: *Peak 10's 9100 square foot Tampa co-location facility is conveniently located near both Interstate 275 and State Road 589 (the Veterans Expressway). Its central location affords fuel replenishment trucks the easy access needed during power outages.*

Proven Track Record: *Peak 10's facility operations continued without interruption during the most recent active Florida hurricane season. The Tampa co-location facility is rated to withstand a Category Three hurricane.*

Redundant Power Sources: *Three Mitsubishi 225 kW UPS systems and a 1500 kW generator provide ample reserve power during local power outages. Peak 10 also maintains an ongoing service contract with local fuel companies in order to guarantee fuel delivery during critical periods.*

Climate Controlled Environment: *Environmental conditions are maintained by an advanced HVAC system for precise room temperature, humidity, and airflow control.*

Fire Safety: *Dual-detection dry-pipe fire prevention system.*

Security Features: *24/7 cardkey access, biometric fingerprint readers, motion/vibration detection equipment, and combination locks on all cabinets provide a superior level of hardware security.*

Site Redundancy: *a network of seven national Peak 10 data centers meets the need for geographic diversity and weather-related redundancy.*

Carrier Access: *Peak 10 has redundant Internet provisions through Level 3, Verizon, and Time Warner fiber networks.*

In addition to the procurement of the co-location facility referenced earlier, NatPay has incorporated several features to address customer concerns related to disaster recovery:

Voice Services: *NatPay has converted to a pure VoIP environment. We utilize a redundant virtual phone/PBX system residing in various locations on the Aptela VoIP System. Our phone and ATA equipment is industry-standard SIP protocol Polycom hardware, and our telephone and telecom capabilities are not location-based. In an emergency, our staff could plug their individual phones into a broadband Internet connection at any co-location, and the phones would locate the virtual circuit and regain all the programming and capabilities of our main office in Tampa. Our customers could still call our main service number and be connected as usual with no service interruption. We could actually relocate our entire office to an offsite hotel without our customers ever noticing the difference – the switchover would be instantaneous.*

Internet Connectivity: *Because the Internet is so vital to our business and our customers, we have devoted significant resources to operational continuity. We maintain a minimum of at least four different pipe types for Internet connectivity. Following is a list of specifications:*

Fiber: *20 MB/s – provided by Verizon Fios*

Fiber: *20 MB/s – provided by Peak 10*

Coaxial: *2* MB/s *– provided by Time Warner Telecom*

NatPay's back-up policy employs several different strategies. All nodes are backed up to hard disk on a nightly basis. Our backup protocol utilizes the most complex blowfish encryption available. In addition to daily tape backups, we back up all server and production data to hard disk devices several times each day, making restoration nearly instantaneous. Finally, we mirror all production storage in real time to a separate location.

Network Architecture and Security

NatPay has many years of experience handling sensitive company information. We understand our customers' need to preserve confidentiality and privacy at all times.

NatPay utilizes time-tested technology in our network topography. Following is a list of information safeguards employed for the security and transport of customer data:

- *Ethernet fully-switched gigabit backbone*
- *Redundancy through multiple Internet pipes/ISPs*
- *Pure non-routable TCP/IP intranet*
- *Enterprise-class AVG virus/malware realtime software on all nodes*
- *Enterprise-class Ipswitch e-mail server with server-level bidirectional Norton antivirus and Declude spam filtering*
- *Industry-leading, managed firewall provided by hardware and other third-party intrusion detection and monitoring software managed by Peak 10*
- *Continuous internal and external vulnerability scans performed by Qualys*
- *All Cisco routers with port-blocking active. Ping and port scans intercepted and blocked*
- *All customer production websites utilize 128-bit SSL3 encryption powered by GeoTrust*
- *PGP encrypted FTP transfers and data files*
- *Linux-based dedicated file servers fully mirrored for dual locations*

Database/File Storage Architecture

NatPay currently employs the SQL database/file storage architecture.

Scalability

NatPay's processing environment was written from the ground up as a fully-distributed group of separate applications. Our innovative design allows any box in our processing pool to lend computing support to any part of our production cycle.

One way in which our system uses this functionality is to process large pay stub customer files. Upon receipt, it determines upon initial examination that the file is a candidate for our distributed pool. This first job then analyzes and breaks the file up into 26 manageable chunks. After the pay stub file is split, the number of outstanding pieces requiring processing trips a threshold flag to alert computers in the distributed pool that assistance is needed. A typical pay stub file passes through no less than 15 independent processing steps on its journey from customer upload to creation of individual stubs that are ready for distribution. Each part of the process can enlist the assistance of additional systems from the pool, with each one adding its weight at an impressive 95% return. This multi-layered approach provides great diversity in our application pool and affords NatPay the luxury of minimal time loss in the event of a job restart. Our corporate commitment to this methodology helps us avoid dependence on larger systems in order to handle peaks in volume and eliminates the existence of any one chokepoint. No single system in our production cycle can malfunction and thereby cause a break in our job flow.

NatPay makes very aggressive service level agreements with our customers. Accordingly, we take our deadline and turnaround times very seriously. Our system processes customer data 24 hours a day, seven days a week in real time. Customers who transmit files at 2 a.m on Sundays receive the same level of processing efficiency and expediency as those transmitting files during standard business hours.

Identity Theft and Data Storage

NatPay was a pioneer in the use of N-tier technology. Our first production website in 1996, Web Direct Deposit, utilized this method to great success.

The first tier is the web server. Its direct Internet connection originally exposed a potential point of compromise. To solve this problem, we essentially made our servers islands unto themselves. They reside on our network, but they're essentially deaf and dumb, having been completely disabled from accessing any machine in the intranet. They do one thing and one thing only. They accept, interpret and translate customer web requests to a central storage location, and then wait for a response. This is where our second tier takes over. It's made up of production applications residing on computers that can see the shared storage location and seek out those requests. This tier is fully distributed in much the same spirit as the rest of our production systems. It interprets and formats the requests before passing them along to the third tier.

The third tier can actually view our production file storage system and access our data. After the information is gathered, it's then passed back down to the second tier for XML formatting. The second tier dynamically generates all of the web pages on our production sites, so there are no static pages to hack and replace.

Summary

We trust that we've addressed many of your questions and concerns in this document. NatPay stands by our commitment to our customers - in fact, many of our leading product innovations were developed as a result of the quality personal relationships that we maintain and our ongoing desire to provide them with the best possible products and service.

Please contact us if you have any questions about the subjects we've discussed here. We welcome your input and will use it for the ongoing enhancement of our technical systems. For more information about NatPay and its offerings, please visit our website at: www.nationalpayment.com.

INDEPENDENT SERVICE AUDITOR'S REPORT

To National Payment Corporation:

We have examined National Payment Corporation's ("National Payment" or the "service organization") description of its Doculivery Online Document Management and ACH Third Party Processing Services system for processing user entities' transactions at the Tampa, Florida, facility throughout the period July 1, 2014, to January 15, 2015, (the "description") and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description. The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of National Payment's controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

National Payment uses Peak 10, Inc. ("Peak 10") for all of National Payment's data center hosting and managed services. The description in Section 3 includes only the control objectives and related controls of National Payment and excludes the control objectives and related controls of Peak 10. Our examination did not extend to controls at Peak 10.

In Section 2, National Payment has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. National Payment is responsible for preparing the description and for the assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria, and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period July 1, 2014, to January 15, 2015.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described in Section 2. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives is subject to the risk that controls at a service organization may become inadequate or fail.

In our opinion, in all material respects, based on the criteria described in National Payment's assertion in Section 2,

a. the description fairly presents the Doculivery Online Document Management and ACH Third Party Processing Services system that was designed and implemented throughout the period July 1, 2014, to January 15, 2015;

b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period July 1, 2014, to January 15, 2015, and user entities applied the complementary user entity controls contemplated in the design of National Payment's controls throughout the period July 1, 2014, to January 15, 2015; and

c. the controls tested, which together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period July 1, 2014, to January 15, 2015.

The specific controls tested and the nature, timing, and results of those tests are listed in Section 4 (the "Testing Matrices").

This report, including the description of the tests of controls and results thereof in the Testing Matrices, is intended solely for the information and use of National Payment, user entities of National Payment's Doculivery Online Document Management and ACH Third Party Processing Services system during some or all of the period July 1, 2014, to January 15, 2015, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

BrightLine CPAs & Associates, Inc.

Tampa, Florida
February 9, 2015