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 Corporation 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, bills with click-to-pay, forms, reports, and a whole lot more!

National Payment and its Doculivery Online Document Management Services are currently Type 2 SAS 70 certified. Please see the INDEPENDENT SERVICE AUDITOR'S REPORT at the end of this document for further information.

Business Continuity Co-Location

National Payment Corporation 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:

SAS 70 Certification: *Peak 10 is a certified Type 2 SAS 70 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, National Payment has incorporated several features to address customer concerns related to disaster recovery:

Voice Services: *National Payment 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: *10 MB/s – provided by Peak 10*

Coaxial: *7* MB/s *– provided by Brighthouse Telecom*

We utilize dynamically-generated TCP/IP addresses, so switching from one provider to another is relatively quick and painless. We have tested switchover time for DNS reassignment for our Web Services and selected a DNS registrar that easily beat the competition. During our last test in August 2006, the DNS reassignment and propagation process took no more than an hour.

National Payment'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

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

National Payment 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

National Payment currently employs the SQL database/file storage architecture.

Scalability

National Payment Corporation'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 National Payment Corporation 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.

National Payment Corporation 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

National Payment 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. National Payment Corporation 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 National Payment Corporation and its offerings, please visit our website at: www.nationalpayment.com.

INDEPENDENT SERVICE AUDITOR'S REPORT

To National Payment Corporation:

We have examined the accompanying description of controls related to the Doculivery Online Document Management Services of National Payment Corporation ("National Payment" or the "service organization") performed at the Tampa, Florida, facility. Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of National Payment's controls that may be relevant to a user organization's internal control as it relates to an audit of financial statements; (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily, and user organizations applied the controls contemplated in the design of National Payment's controls; and (3) such controls had been placed in operation as of December 31, 2009. National Payment uses Peak 10, Inc. ("Peak 10"), an independent service organization that provides data center services to National Payment, applicable to the Doculivery Online Document Management Services of National Payment. The accompanying description includes only those control objectives and related controls of National Payment and does not include control objectives and related controls of Peak 10. Our examination did not extend to controls of Peak 10's data center services. The control objectives were specified by the management of National Payment. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

In our opinion, the accompanying description of the aforementioned Doculivery Online Document Management Services presents fairly, in all material respects, the relevant aspects of National Payment's controls that had been placed in operation as of December 31, 2009. Also, in our opinion, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and user organizations applied the controls contemplated in the design of National Payment's controls.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific controls, listed in Section 3 (the "Testing Matrices"), to obtain evidence about their effectiveness in meeting the control objectives, described in the Testing Matrices, during the period from July 1, 2009, to December 31, 2009. The specific controls and the nature, timing, extent, and results of the tests are listed in the Testing Matrices. This information has been provided to user organizations of National Payment and to their auditors to be taken into consideration, along with information about the internal control at user organizations, when making assessments of control risk for user organizations. In our opinion, the controls that were tested, as described in the Testing Matrices, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in the Testing Matrices were achieved during the period from July 1, 2009, to December 31, 2009.

The relative effectiveness and significance of specific controls at National Payment and their effect on assessments of control risk at user organizations are dependent on their interaction with the controls and other factors present at individual user organizations. We have performed no procedures to evaluate the effectiveness of controls at individual user organizations.

The description of controls at National Payment is as of December 31, 2009, and information about tests of the operating effectiveness of specific controls covers the period from July 1, 2009, to December 31, 2009. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specific controls at National Payment is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected.

Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such conclusions.

This report is intended solely for use by the management of National Payment, its user organizations, and the independent auditors of its user organizations.

SAS 70 SOLUTIONS

January 29, 2010