



CASE STUDY



NetSpend Corporation

The Nation's Leading Processor of Prepaid Debit Cards Uses VeriSign for its PCI Data Security Standard Assessment



Where it all comes together.™

NetSpend Corporation

SOLUTION SUMMARY

Totally dependent on maintaining a current Payment Card Industry (PCI) certification, NetSpend turned to VeriSign to perform the PCI Data Security Standard assessment. It was successfully accomplished in a short time period, meeting NetSpend's deadline, without causing any business interruption.

Industry

- Financial Services

Challenges

- NetSpend needed to substantiate its compliance with the PCI Data Security Standard via an independent assessment.
- The company did not want the PCI assessment process to negatively impact daily operations.
- NetSpend needed to complete the PCI by a specific near-term deadline.

Solution

- VeriSign® Global Security Consulting for the PCI Data Security Standard assessment.

Results

- By passing the PCI DSS assessment and remaining PCI compliant, NetSpend can continue to grow its business and expand into new markets with innovative and exciting product lines.
- A three-week assessment was reduced to four days, and it was completed ahead of the target date because of NetSpend's thorough preparation and VeriSign's expertise and efficiency.
- VeriSign completed the assessment without interrupting NetSpend's business operations.

NetSpend Corporation is an issuer and processor of prepaid MasterCard and Visa payment cards specifically catering to customers with limited or no access to banking services. Often referred to as the “unbanked” or “underbanked” segment, it is in fact a very large population for whom NetSpend provides an invaluable set of services.

Denis Brooker, NetSpend's information security manager, explained, “We provide the full suite of processing services ranging from account acquisition to customer service to risk management. When a NetSpend customer uses their card to pay for an item, that transaction is directed to our systems to determine if the person has enough funds available for the specific purchase, and then returns the appropriate ‘accepted’ or ‘declined’ code back to the merchant. We have become the nation's leading processor and marketer of prepaid, re-loadable debit cards, as well as being the fastest growing.”

+ Needing to Pass a PCI Data Security Standard Assessment

The Payment Card Industry (PCI)—including Visa, MasterCard, Discover, and others—has come together to establish the PCI Data Security Standard (DSS), which mandates that any company that processes, stores, or transmits credit card data must comply with the PCI-DSS stipulations. The requirements encompass building and maintaining a secure network; protecting cardholder data; operating a robust vulnerability management program; implementing strong access control measures; regularly monitoring and testing networks; and maintaining an information security policy.

NetSpend's compliance with PCI regulations is a demonstration of its ability to offer the convenience of prepaid debit cards securely, so while NetSpend is audited by many different entities during the course of standard business practices, one of the most critical examinations is the PCI assessment to ensure compliance with the Data Security Standard.

PCI has characterized all of its constituent companies by type as well as by volume of transaction processing. Using these groupings, the PCI has assigned levels, from largest (Level I) down to smallest (Level IV). Based on its designated level, a company must perform a pre-defined series of tasks to substantiate compliance with the PCI Data Security Standard.

“MasterCard and Visa are a significant component of our business, so everything that we do has PCI implications,” stated Brooker. “We worked with Visa on our PCI requirements and determined that we were to be a Level I Service Provider, meaning we would have to undergo annual onsite assessments and penetration testing, in addition to quarterly scanning. As the information security manager, I am responsible for coordinating all of these activities.”

Brooker started by thoroughly reviewing the PCI documentation to understand exactly what the assessors would be requiring for review. He had concerns about the impact of the assessment process, “The pace of our day-to-day operations is very fast, so it was important to us that an assessment should not be too burdensome or cause too much interference.



+ Selecting an Assessor

The search for a PCI assessor was initiated by Brooker with a review of the listing of qualified assessors certified by the PCI Security Standards Council (PCI SSC). “We looked at the bigger players in the market because it was important to us that we work with a qualified organization and one with a widely recognized name,” said Brooker. “In addition, we were searching for a company that could demonstrate solid assessment experience.”

NetSpend issued a request for proposal for an onsite Level I assessment that asked responders to address very specific questions about past customers, and the scope and size of those PCI assessments. “We followed up with some of the references that were provided, and got a good feel for how well the assessors worked with each company,” recalled Brooker. “We invited three of the contenders to come onsite and we continued questioning them; discussing a variety of objectives, alternate methodologies used during the assessment, and timeframes.”

VeriSign was one of the first assessors to conduct PCI onsite audit and scanning services under the Visa Cardholder Information Security Program (CISP) and MasterCard Site Data Protection (SDP) initiative. VeriSign leverages regulatory knowledge, training, and experience; best-of-breed solutions; a digital infrastructure that is intelligent, highly scalable, and secure; and its history of stability to help companies appropriately and cost-effectively address PCI requirements. The VeriSign® Global Security Consulting practice was one of the first providers of onsite assessments for both Visa and MasterCard, and is a designated Qualified Security Assessor (QSA) by the PCI Security Standards Council, LLC. Since the program’s inception, VeriSign has conducted several hundred assessments for some of the industry’s largest merchants and service providers. Today, VeriSign has the most QSA certified consultants in the industry.

The VeriSign Global Security Consulting practice was chosen by NetSpend to conduct its PCI DSS assessment. “We selected VeriSign based on several factors, one of which was its name recognition,” noted Brooker. “VeriSign is a big player in the security market and we were impressed that we were able to partner with a company of that stature to conduct our assessment. We liked its methodology, how long it was going to take to do the assessment, and its ability to start at relatively short notice and meet the requirements for completing the assessment within our specific timeframe. All of these came into line and really pointed out very clearly that VeriSign was the correct company with which to work.”

+ Making the Assessment Process Painless

NetSpend benefited from Brooker’s extensive knowledge of information security nuances. “The PCI assessment is very much about a company’s policies and procedures, and how those are recorded. In going through the PCI DSS documentation we found some very intricate details that could be overlooked if one didn’t fully understand the security space,” reflected Brooker. “We were pleased to find we already were doing things correctly, and we had documentation to back it up.”

An onsite PCI assessment performed by VeriSign Global Security Consultants consists of interviews with key personnel; investigation of policies, procedures, and associated documentation; an architecture review; vulnerability testing; and examination of key device configurations. The result of this effort is a ‘Report of Compliance’, which articulates the company’s adherence to the PCI Data Security Standard.



CASE STUDY

“The PCI assessment is the most important checkpoint that we go through on a recurring basis. The fact that VeriSign was able to come in and assist us with this, and do the assessment in such a short time period without causing any business interruption, was a huge benefit.”

Denis Brooker
Information security manager
NetSpend Corporation

“The two VeriSign PCI experts that came in were very professional,” recounted Brooker, “they really understood the industry and what it is that they needed to do to complete this assessment without interrupting our daily operations. On arrival they gave us a listing of what was to be reviewed and we were able to provide all necessary documents. They engaged in an intense period of study as they examined all of our different information security policy documents. Then they moved to reviewing compliance with system requirements, including components such as firewalls.”

Having gone step-by-step through the PCI requirements, NetSpend was well prepared for the arrival of the VeriSign assessors, and had proactively sent a listing of the items they would be evaluating. “The listing was pretty much right on target,” Brooker said, “so although it was originally intended to be a three-week assessment, our preparation and collaboration allowed us to reduce it to four days.”

+ Performing Perfectly

Brooker’s impression of the VeriSign assessors was that they were very proficient and exceptionally thorough. He said, “They knew exactly what they needed to see, and were highly efficient in evaluating each item for compliance. So it was an extremely good experience from our perspective and we were very happy with them. I cannot think of a single thing that I would’ve changed as far as the process of selection and their ability to respond. Everything that VeriSign did as far as was spot-on—the consultants performed pretty much perfectly.”

NetSpend was immensely successful in meeting PCI compliance because of its advance preparation for the assessment. From its executive management and board, down through the senior management, to every individual director and manager, the PCI assessment was given top priority. “The support from a management perspective was phenomenal, making my job a lot easier. I didn’t have to fight to get PCI-related tasks executed with appropriate urgency; it had the priority that it needed,” remarked Brooker.

In reflecting on the experience, Brooker noted, “Complying with the PCI DSS is a matter of being able to appropriately monitor your environment and having the ability to prove that the monitoring is being performed in a rigorous and consistent manner. To anyone embarking on a PCI assessment I would recommend that they perform a self-audit by reviewing the documentation that shows what the assessor is going to look for. If the company is already complying with the requirements, it obviously has a viable security posture, and has a good shot at passing the assessment the first time.”

Brooker summarized, “We are growing at such a phenomenal rate—including rolling out new products and signing up new partners—that we are totally dependent on maintaining a current PCI certification. Consequently the PCI assessment is one of the most important checkpoints that we go through on a recurring basis. The fact that VeriSign was able to come in and assist us with this, and do the assessment in such a short time period without causing any business interruption, was a huge benefit. By remaining PCI compliant, we are excited to be able to continue to grow our business and expand into different markets with new, innovative product lines.”

Visit us at www.Verisign.com for more information.

©2007 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, “Where it all comes together.” and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign and its subsidiaries in the United States and in foreign countries.

00024357 03-16-2007