Leveraging a Secure IP-Based Payment Connection Network to Reduce Costs and Increase Customer Satisfaction

Merchants can reduce payment network access costs while enhancing customer satisfaction, increasing security and lowering other expenses.

By Souheil Badran, SVP and Division Manager, eCommerce Solutions and Dan Skowronek, Senior Director, Product Management, Secure Transport

© 2009 First Data Corporation. All trademarks, service marks and trade names referenced in this material are the property of their respective owners.
Introduction

The ubiquitous card swipe has been a familiar feature of commerce for decades. For consumers, it’s a daily activity that’s become part of our modern culture and shopping routine. According to a 2008 study by Hitachi Consulting and BAI, payment card transactions now comprise over 63 percent of in-store purchases—a figure that has risen steadily over the past decade and is expected to continue to increase.1 Whether we are swiping our card at a gas station, grocery store or specialty retailer, we take this frequent and consistent activity for granted.

Merchants look at it differently, though. For them, the card swipe kicks off a burst of activities and processes that eventually result in cash flow, but can also lead to unnecessary expenses and fraud. While consumers take the safety and consistency of card swipes for granted, savvy businesses are constantly looking for ways to protect these transactions and make them faster, less expensive and more secure. What they’ve found is that the Internet is not only the most cost-effective method for transporting payment card transaction data, but can also be the safest when combined with solutions from industry-leading service providers.

Internet Protocol (IP) technology has been around for years. It is used extensively for most forms of digital communications, ranging from sophisticated high-definition cable television and videoconferencing applications to Web browsing and e-mail. Yet, only in the last few years has it become practical for merchants to use IP functionality at the point-of-sale (POS) as a way to access payment networks for transporting payment card data.

Most of the largest merchants made the switch from legacy dial-up POS systems to IP years ago. This initial migration occurred relatively rapidly because the “benefits of IP in terms of speed and integration to the cash register and back-end systems” were simply too compelling to ignore, according to Mercator Advisory Group.2 IP adoption at the point-of-sale among the six million small to medium U.S. retailers has been considerably slower, however. As of January 2009, over 60 percent of the POS terminals in the United States still accessed payment networks using a dial-up modem.3 According to industry journal The Green Sheet, the reluctance to make the switch stems largely from inertia: dial-up technology is familiar, reliable and already in place—so why change anything?4

Many merchants are also hesitant to make the investment in upgraded POS equipment needed to support IP transport. Merchants may also be apprehensive about the shared nature of the Internet, which “invokes the specter of bandwidth hogs, hackers, fraud risk and non-compliant behavior regarding PCI.”

A new generation of IP transport solutions may change these merchants’ minds—and may also prove appealing to merchants that have already switched from dial-up to a conventional IP network solution. Next-generation IP solutions offer significant advantages over dial-up POS network connectivity, while addressing the inherent issues with transmitting data over the public Internet. With the proliferation of inexpensive broadband connectivity, most retailers already have Internet access connections on premise. These DSL, cable, modem or T1 broadband connections can be used to simultaneously carry payment processing data. So businesses can now access IP payment networks at little or no incremental cost, and may even save money by terminating their dedicated POS dial-up modem lines. This paper discusses the benefits of migrating to a proven next-generation, secure IP-based payment connection network for transporting transaction data, and explains why merchants cannot afford to wait any longer to adopt this cost-effective, secure and reliable Internet technology.

**Accessing Payment Networks Conventionally**

Until the recent emergence of secure IP-based payment connection networks, there were four primary ways for merchants to access payment networks or payment gateways.

**Dial-up Modem and Phone Lines.** For decades, this was the simplest and cheapest way of accessing payment networks: using standard lines from the phone company to send and receive transaction data using a dial-up modem. For the merchant, the cost of purchasing a dial-up POS terminal is extremely low, and both installation and configuration are quick and simple. However, advantages in other technologies have now rendered this a comparatively slow and expensive payment network access method. With the cost of a dedicated dial-up phone line averaging between $40 and $70 per month, annual costs of using this transport method range between $480 and $840 a year, per line.

**SSL Gateways.** For merchants wishing to leverage IP technology to access payment networks, the easiest and least expensive method has been to use a new or existing broadband connection (e.g., DSL, cable, T1) to transmit data via an SSL gateway. SSL is an acronym for Secure Sockets Layer, which is a widely used encryption methodology that provides a secure link between two locations. In this method, the merchants’ IP-enabled POS terminals encrypt the transaction data using SSL protocols and transmit the encrypted data over the public Internet to payment processors and acquiring banks through an SSL gateway that unencrypts the data for processing. While SSL is reasonably secure, it is not foolproof. The weak points for most SSL gateways are a lack of redundant routing paths and vulnerability to major Internet disruptions. The cost for accessing payment networks using this method varies depending on the type of broadband connection the merchant uses; an entry-level broadband connection can be obtained for as little as $25 a month.

---

Virtual Private Networks (VPNs). Widely used in corporate data networks, VPNs allow merchants to use the Internet to access payment networks by effectively turning the public Internet into their own private networks. By doing this, they gain added security and control of the Internet, but this requires expensive routers and more IT overhead at each point in the “private” network. VPNs make the most sense for large businesses with ongoing and point-to-point data needs. The average annual cost for using a VPN to access payment networks varies widely between $1,200 and $12,000 per location, depending on specific data needs.

Leased Lines and Frame Relay. Also widely used in corporate data networks, leased lines and frame relay allow merchants to set up high-volume, point-to-point dedicated IP-based data connections. By doing this, they gain increased security and control, but like VPNs, this also requires routers and additional IT resources. In addition, merchants pay premium service fees to telecom operators for these dedicated data connections. The average cost for using a leased line or frame relay to access payment networks varies based on many factors, ranging between $1,200 and $12,000 per year for each location.

These payment network access methods adequately transport data for millions of payment card transactions every day. But as you are about to discover, secure IP networks have some significant advantages over these legacy methods. Migrating to a secure IP-based payment connection network (also known as a secure IP network) could result in saving a few hundred dollars a year in communications expenses for a small merchant, to tens of thousands of dollars annually for a large, multi-location merchant. It also offers significant gains in speed, reliability and security that may result in revenue gains and further cost reductions.

Advantages of Using a Secure IP-Based Payment Connection Network

A secure IP-based payment connection network from a trusted provider offers many compelling advantages over old-fashioned dial-up network access. It even provides some incremental benefits over conventional types of IP-based solutions such as virtual private networks, leased lines, frame relay and others.

Speed. Perhaps the most glaring drawback to using a dial-up modem to access payment networks is the sluggishness of transmitting data. The time it takes to authorize a payment card transaction using dial-up ranges, on average, between 10 and 20 seconds. Compare this to the two to four seconds it takes to authorize a transaction using an Internet payment network access method such as an SSL gateway, VPN, leased line or frame relay. With a secure IP-based network, this figure can be even faster, due to the optimal path routing utilized by that type of solution.

The difference in authorization time may seem trivial at first glance, but it can have a profound effect on a merchant’s success. Consider this survey data from M/A/R/C Research on the impact of customer wait times at retail stores: 43 percent of shoppers indicated that long lines would influence their decision to shop at a particular store in the future. According to The Green Sheet, as few as five or 10 customers in the space of an hour can result in queuing at the checkout stand. Wait times can add up quickly when transactions are being authorized using slow dial-up technology, resulting in displeased customers and lost sales. In fact, M/A/R/C Research’s study revealed that 10 percent of shoppers become frustrated enough to leave a checkout line if their wait is more than four minutes, and three percent will never return to the store.

Disturbingly, for merchants relying on dial-up payment network connections, delays of just a few seconds on each transaction can result in thousands of dollars of lost sales each year. The improved transaction speed and reduced wait times imparted by IP functionality not only enhance customer satisfaction, they also increase labor efficiency, potentially reducing employee expenses during peak times.

**Cost.** According to Nielsen, nearly 97 percent of Americans have access to broadband Internet connections in the workplace, suggesting that most merchants already have high-speed Internet connectivity in place.\(^8\) If this is the case for a particular merchant, there is no incremental monthly cost for sending transaction data over the existing broadband connection. In fact, the merchant will save money because it can subsequently eliminate the dedicated phone line used for dial-up data transmission. Merchants can potentially save even more on their communications expenses by switching their voice phone lines to lower-cost Voice over Internet Protocol (VoIP) lines that use their existing broadband connections.

If a merchant uses POS terminals that are not IP enabled, it will need to upgrade to new terminals—however, according to Mercator Advisory Group, this expenditure is “recovered very quickly” with the expense of the POS terminal offset in just a few months by the cost saving from dropping the superfluous phone line or lines. With millions of POS terminals expected to become non-compliant with PCI standards in 2010, this is the perfect time for many merchants to upgrade their equipment, if necessary, to technology that is both compliant and IP enabled. The business case for investing in new POS equipment is further enhanced by the dramatic growth of PIN debit transactions—which are not supported by many legacy POS terminals. Investing in upgraded IP-enabled terminals that also support PIN debit transactions may potentially improve customer satisfaction (by providing a highly sought-after payment choice) as well as reduce interchange expenses (because interchange rates on PIN debit transactions are generally lower than credit or signature debit transactions).

In addition to reducing communications expenses, converting to a secure IP network can also save merchants money on transaction processing fees. According to industry data, the fees charged by acquirers to authorize dial-up transactions are as much as 20 percent higher than the fees for authorizing IP-based transactions. Moreover, The Strawhecker Group’s annual merchant processing pricing benchmark study indicates that IP authorization costs are decreasing dramatically faster than dial-up authorization costs.\(^9\) Converting from dial-up to IP allows merchants to take advantage of this pricing differential, and could save them hundreds or even thousands of dollars a year, depending on their transaction volume.

For merchants that are using IP network access methods such as virtual private networks, leased lines or frame relay, switching to a more cost-effective secure IP-based payment connection network can offer substantial savings by eliminating the need for costly dedicated connections, expensive routers and network access equipment—not to mention enabling a reduction in IT and network management expenses.

---

\(^8\) Nielsen Online, September 2008.

Security. Dial-up POS terminals generally do not provide any security for transaction data in transit, based on the supposition that a criminal would have to tap into individual phone lines to intercept the data—generally a difficult undertaking with limited payback. While rare, dial-up transmission breaches do occasionally happen. Conventional IP-based transactions use SSL encryption to protect data, but this does not “confer huge improvements in security,” according to Mercator Advisory Group. Secure IP-based payment connection networks address the inherent security vulnerabilities of the Internet by deploying sophisticated embedded authentication and encryption technology. These measures safeguard transaction data in transit far more effectively than standard SSL, providing enhanced protection against hackers and data breaches. Furthermore, utilizing a secure IP network to transport payment data may also reduce a merchant’s PCI compliance burden.

Reliability. Dial-up payment network access is generally very reliable; however, merchants that have adopted conventional forms of IP network access sometimes experience downtime due to Internet disruptions and network outages. Secure IP-based payment connection networks are less prone to denial-of-service attacks and other types of systematic disturbances. In addition, some secure IP network solutions provide automatic failover in the event the merchant’s broadband connection goes down—meaning that it will immediately begin transmitting payment data via a dial-up Internet service provider (ISP) until broadband Internet connectivity is restored.

How a Secure IP-Based Payment Connection Network Works

In response to merchants’ needs for an easier, safer and more cost-effective method of accessing payment networks, technology providers have developed secure IP-based payment connection networks—sophisticated transaction delivery networks that “overlay” the public Internet.

It’s important to note that a secure IP-based payment connection network is not a payment gateway or payment processing solution. At its simplest, it is a merchant-connectivity option that safely and speedily delivers merchant transaction traffic to payment processors. Unlike payment gateways, it does not provide payment pages, virtual terminals, or POS payment formatting applications. It is simply a way to access payment networks from multiple points using the low cost and widely available Internet. In doing so, the secure IP network:

→ Leverages the strengths of the public Internet, especially its widespread availability and cost-effectiveness
→ Addresses the weaknesses of the public Internet, including security, performance and consistency

A secure IP-based payment connection network allows merchants to use an existing or new broadband Internet connection (cable, DSL, satellite or wireless) to transmit and receive transaction data. Via any ordinary broadband Internet connection, merchants access the network at entry points strategically distributed across the globe. Multiple access points allow merchant POS terminals to identify the fastest path into their particular payment networks and provide multiple alternative entry points in the case of Internet traffic disruptions.

One of the most important features of a secure IP-based payment connection network is that every transaction is authenticated as it enters the network, before it is routed on to the intended processor. First Data’s secure IP payment connection network solution, Secure Transport, supports more than 150 approved POS devices and payment terminals—and each one contains embedded code, along with unique data points, that provides the authentication credentials for every transaction allowed into and transmitted across the network. Thus, all communication between merchants’ point-of-sale payment applications and the network is encrypted with at least 128-bit SSL, Triple DES or AES encryption, with a unique key for each transaction. For those devices that do not contain embedded code, special hardware interfaces can be provided that convert legacy or non-IP terminals into fully secure IP communication devices—minimizing the required investment in new POS hardware. By authenticating at the device and transaction levels, an effective secure IP network essentially builds a moat around the payment processing information, making it the most secure transport option available to merchants.

Once a transaction accesses the secure IP network, multiple switching nodes use least-cost/fastest-path routing algorithms to provide the best path to the payment processor. The multiple nodes also provide redundancy and create a “self-healing” network in the event of hardware or other outages. First Data’s Secure Transport solution, which was formerly known as Datawire, has been in service for eight years and has never experienced a network outage. Even during periods of major Internet backbone failures, such as those experienced during the East Coast power outage of 2004 and various recent Internet worm attacks, the Secure Transport network has not experienced even the slightest performance degradation.

In the prototypical secure IP network architecture, there are three types of nodes or connection points. First, edge nodes regulate access to and from the Internet into the secure IP network. The edge nodes interface with the merchant and are accessed by compliant POS applications and devices connected to the Internet via any Internet access method. Next, core nodes act as traffic directors within the secure IP network, facilitating the optimum route for a transaction, based on the traffic and load of the underlying Internet backbones. Finally, service nodes provide a secure and dedicated connection to the payment processor’s infrastructure, and insulate the payment processing hosts from direct Internet connections.
While a secure IP network solution may look and sound complex, its design is actually remarkably straightforward: it is simply a network that “overlays” the public Internet using secure, redundant co-location facilities. This distributed architecture enables it to deliver reliable and consistent performance—indeed, independent of the underlying condition of the Internet. It also allows it to take advantage of the ubiquity and cost-effectiveness of the Internet, while alleviating some of its inherent security risks.

Conclusion

In an industry where checkout speed is a critical factor in customer satisfaction and operational efficiency, slow dial-up transactions can seem like an eternity and can lead to lost sales and increased labor costs. With the additional presence of security threats and compliance hurdles, it is essential that merchants adopt a payment network access method that is fast, cost-effective, reliable and secure. Merchants simply cannot afford to do otherwise. If a merchant has access to broadband Internet connectivity, “there’s absolutely no reason—physical or financial—why the POS shouldn’t be converted” from dial-up to IP, according to The Green Sheet. Given the potential security and reliability issues associated with transmitting payment data across the public Internet, merchants need to consider using a secure IP network to transport transaction data.

In the face of stagnant or declining sales volumes, merchants must do everything possible to maintain customer satisfaction and market share while reducing costs. With the continued rise in payment card usage, dial-up authorization delays at the POS will become only more pronounced, and customer displeasure with wait times will increase. Merchants can also not afford brand deterioration and lost sales from data breaches or data transmission failures. Fortunately, adopting a secure IP network solution provides merchants with the opportunity to reduce wait times, increase security, improve reliability and shrink expenses.

Most merchants can start saving money and sending more secure transactions right away. The first step is to call your payment processor. Many have access to reliable and cost-effective secure IP network solutions like First Data’s Secure Transport, and can easily facilitate the service. The capability to access these networks is already built into most popular POS systems and payment terminals, and there are also “emulation” solutions available that enable the networks to work with legacy equipment that traditionally used dial-up or VSAT satellite systems to access payment networks.

Secure Transport provides services for thousands of retail merchant locations. Regardless of your existing POS systems—whether they are non-IP capable, IP terminals, PC-POS software or other eCommerce solutions—Secure Transport most likely offers a certified solution for you. Currently, there are more than 150 compliant POS vendors certified to securely access the network, with a combined 450 POS and terminal certifications spanning multiple acquiring processors. In 2008, the Secure Transport network transported nearly 1.9 billion transactions, handling a monthly volume often exceeding 150 million transactions while servicing more than 100,000 satisfied merchant locations.
About The Authors

Souheil Badran leads First Data eCommerce Solutions as Senior Vice President and Division Manager. He joined First Data in January 2008 with extensive experience in high-technology organizations including sales and marketing; product management; strategic development; mergers and acquisitions; and high-growth initiatives. Prior to First Data, Badran served as president and general manager at Rebtel, where he was responsible for driving Rebtel’s growth strategy and operations in the Americas and APAC. Before joining Rebtel, Badran held senior management positions at VeriSign, Digital Insight and Metavante.

Badran serves on the board of trustees for Cardinal Stritch University and is on several technology advisory boards. Badran received his MBA in marketing and undergraduate degree in computer studies from Cardinal Stritch University in Milwaukee.

Dan Skowronek is a Product Management Director for Secure Transport in the eCommerce group. Skowronek joined First Data in April of 2003 with extensive experience at organizations serving merchant needs, including positions in organizational leadership, product management and strategic development. Skowronek currently has over a dozen pending patent applications with First Data across a diverse range of payment solutions, from contactless to interchange management.

Prior to First Data, Skowronek co-founded Yclip.com, a company that empowered merchants to distribute loyalty offers to customers over the Internet and then automated offer redemption through the credit card settlement process. First Data was an early investor in Yclip and fully acquired the company in 2003. Skowronek received an MBA from the University of Texas at Austin.

For more information, contact your First Data Sales Representative or visit firstdata.com.