COMPLETING THE PAYMENT SECURITY PUZZLE

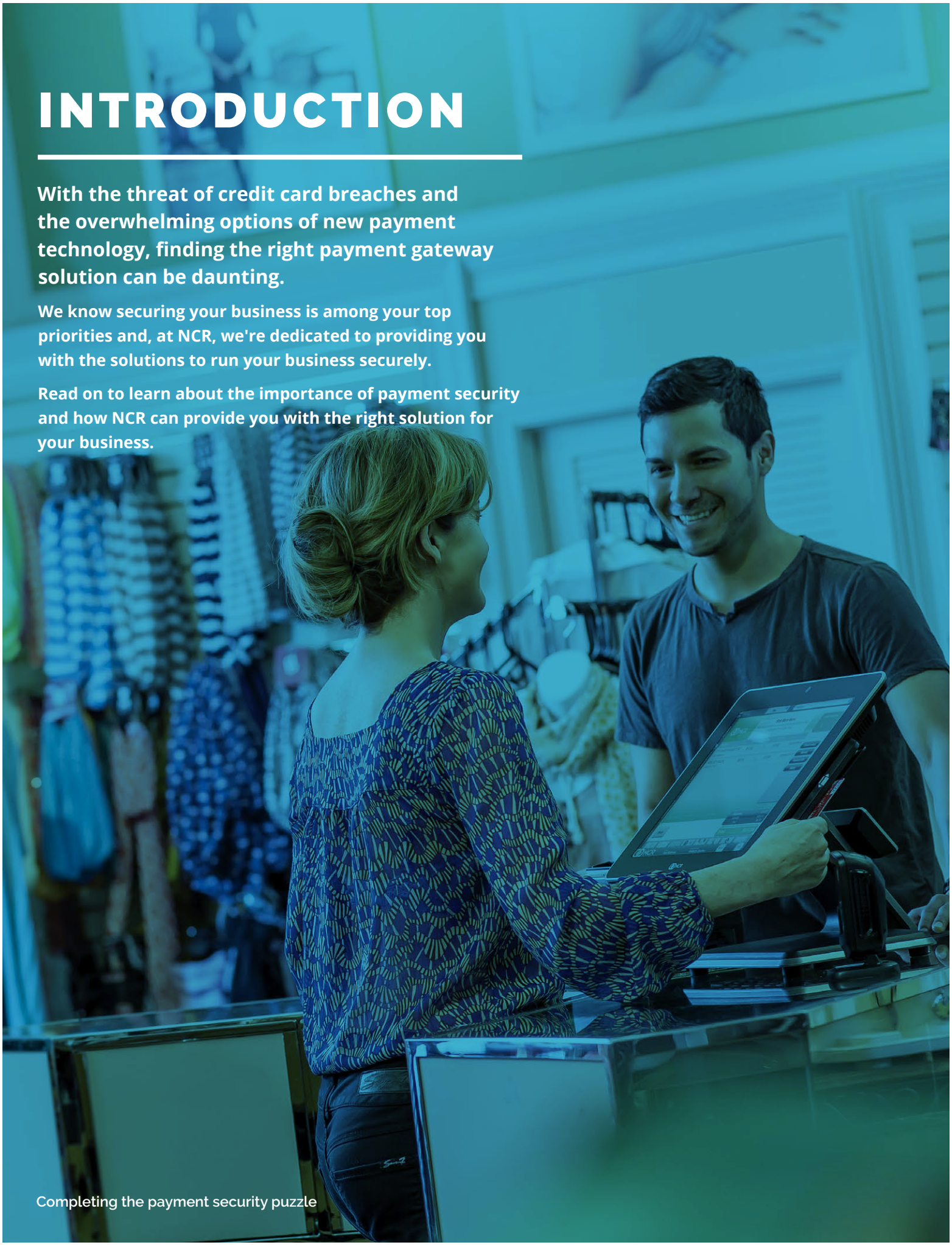
An NCR white paper

INTRODUCTION

With the threat of credit card breaches and the overwhelming options of new payment technology, finding the right payment gateway solution can be daunting.

We know securing your business is among your top priorities and, at NCR, we're dedicated to providing you with the solutions to run your business securely.

Read on to learn about the importance of payment security and how NCR can provide you with the right solution for your business.



1. IMPORTANCE OF PAYMENT SECURITY

Big box stores aren't the only ones affected by security breaches; retailers of all sizes need to be aware of how to protect their business. Credit card data breaches are expensive — even a modest exposure of 50 customer credit card numbers can result in unplanned costs of $10,0001 or more in penalties, fees, time expenditure, and, the most difficult to quantify: reputation.

Navigating the payment security world with buzzwords like Point-to-Point Encryption, Tokenization, and EMV can feel overwhelming.

We want to help you put together the payment security puzzle to keep your customers' payment information protected.

1-Focus on PCI – Penalties Calculator: http://www.focusonpci.com/site/index.php/Penalties-Calculator.html

2. LAYERS OF RETAIL PAYMENT SECURITY

There's no silver bullet solution to guarantee protection against a payment security breach. A layered approach is necessary to create a more secure environment to transmit credit card information. Both perimeter security and safeguarding payment information play a role in creating a secure environment.

Creating a Secure Perimeter

You can't be secure if unauthorized users can gain access into your system network and machines. Creating a secure IT perimeter is your first step and you can start by adding a firewall. A firewall will not catch everything; it's simply a first line of defense at the perimeter of your network.

Your next step is to install antivirus software, keeping in mind that outdated antivirus software is as much of a threat as not having any. After installing a firewall and anti-virus, make sure to whitelist the web sites and applications you use. Malware cannot infect machines if the code cannot be run. By whitelisting the web sites and applications that are allowed to run, you essentially shut down everything else.

Your next line of defense is to require complex passwords. We all hate typing iH8Pwd5 to log onto our machines, but we should do it, regardless. PCI standards dictate a 7 character password with 3 of the following t characteristics:

- upper case letters
- lower case letters
- numbers
- special characters.

It's fairly simple to make a complex password that's still easy to remember. The one you just read is short for "I Hate Passwords." This sort of password is recognizable as a pattern but difficult to crack.

Utilize network segmenting. If you provide your customers with Wi-Fi access it is important to keep that Wi-Fi separated from the POS segment of the network.

Finally, ensure that the remote access tools that system administrators use to support the system are not used as an entry point for unauthorized users. For example, ensure that remote access tools are not configured to remain in "listening mode" on the site system, and that remote access must be initiated from inside the site system. Other remote access control recommendations include using two-factor authentication (something you have, like a code sent to your cellphone; and something you know, like your password) for access, and to log all access and activities by remote personnel.

Setting up these layers of network security will help you filter out threats that exist today.

Safeguarding Payment Information

When it comes to securing the card data itself, there are 2 main elements to consider: data storage and the transmission of data.

Data Storage

The way card information is stored in your retail location is a key component of security. You need to ensure that you are storing cardholder information securely at all locations in your retail environment.

THERE ARE MANY WAYS TO STORE SENSITIVE INFORMATION:

Masking truncates the card data by putting X's in the middle and deleting the full length card number. This is good for reporting and looking up transactions or customers using the credit card number; however, it does not allow you to do subsequent transactions, like returns, without asking for the payment card again.

Encryption uses advanced encrypting techniques to keep sensitive data in your system in a concealed manner. This allows you to reuse card information for other transactions, including returns. The only downside to encryption is that, in the unlikely event that someone gets your encryption keys, they would be able to access full card data.

The most secure method of data storage is tokenization, also known as token replacement. Tokenization stores a token instead of an actual card number. If your system were breached, unauthorized users would only find the token information and not the actual card information, since the card information is stored in a token vault. With the token, you can access the transaction information as needed for returns and other operations, including card on file billing, while maintaining a secure system.

Transmitting Data

Transmission of cardholder data between your system and the payment processor can be an area of weakness that cyber payment criminals target.

To get an approval from a credit processor, card information must travel from the MSR (card reader) through the Point of Sale (POS) application and operating system (OS) to an application which communicates with the credit processor in order to get an authorization. Most systems pass the card data from the MSR unencrypted through the OS to the POS application and encrypt before sending the approval communication to the credit processor.

Point-to-Point Encryption (P2PE) goes beyond encrypting solely during the transmission to the credit processor and encrypts directly by the MSR hardware from the time the card is swiped. The encryption happens in the hardware on the MSR device, not inside your system, and unencrypted data does not exist on your POS network. Thus, sensitive cardholder information is encrypted throughout its lifecycle in your environment, reducing your risk of an unauthorized user scraping the data from memory.

Another difference worth noting with P2PE as compared to traditional encryption is that the encryption and decryption processes use different keys. Even if you have the encrypting key, you can't decrypt the data because key to unlock the data is not the same

3. NCR'S SOLUTIONS

NCR Network Security Services

A suite of managed products to optimize your IT operations and safeguard your data.

NCR created the Network and Security Services (NSS) team to help you manage and secure your IT perimeter through ongoing oversight and tuning. Rather than merely taking a single action that temporarily addresses an issue or deploying a single tool that only partially addresses your needs, our NSS team sets up tools at your location that allow them to oversee and take care of your network and the systems connected to it, so you can focus on running your business.

NSS IS A SUITE OF MANAGED PRODUCTS AVAILABLE AS A SET OR INDIVIDUALLY. THE CORE COMPONENTS OF THE NSS SOLUTION SET ARE DESCRIBED BELOW:

Site Shield

This commercial-grade multi-featured firewall enables network connectivity in a controlled manner. Site Shield restricts dangerous connections to and from the Internet while allowing the necessary business applications to function. This helps defend against network-borne malicious software and attacks, especially as they pertain to payment and other sensitive systems. Moreover, Site Shield provides reliable wired and wireless connectivity within the site.

Threat Defender

This modular agent helps create reliable operation of systems within the site. Installed on both payment-processing terminals and other PCs, Threat Defender scans your systems for common security weaknesses. It can also control what applications may or may not run - "whitelisting" - to minimize disruptions due to a virus infection, a network compromise or a self-inflicted problem. Threat Defender can also optionally update commonly-exploited applications to further safeguard the system on which it is installed.

Secure Access

This tool provides a trusted way of accessing systems over the Internet. It offers a reliable alternative to the insecure remote access setup often employed by organizations and exploited by cyber criminals. Secure Access provides remote control and file transfer capabilities to and from the main site computer. It encrypts and logs its connections and restricts access to designated people. It also includes two-factor authentication for stronger security.

PCI Compliance Services

This value-added component will assist you with your PCI DSS compliance requirements by providing a web-based "wizard" for answering the PCI self-assessment questionnaire. It also conducts quarterly external PCI-mandated network scans, offers an information security policy builder, and includes on-demand security awareness training you can provide to your employees.

4. NCR SECURE PAY

A PCI-DSS Compliant and Secure Electronic Payment Gateway

NCR created an electronic payment gateway, NCR Secure Pay, to help minimize your risk for a credit card security breach by addressing the two key elements of payment security: data storage and data transmission.

We take the storage of sensitive card information out of your local system and move it to our NCR Secure Pay host while using Point-to-Point Encryption to help secure sensitive information during transmission.

NCR Secure Pay was built to allow you to process payments in a PCI-DSS compliant manner with high levels of security. This hosted electronic payment gateway works with our retail management software solution, NCR Counterpoint, and integrated eCommerce tool, NCR Retail Online, for credit cards, debit cards, and stored value cards (gift cards).

Token Replacement

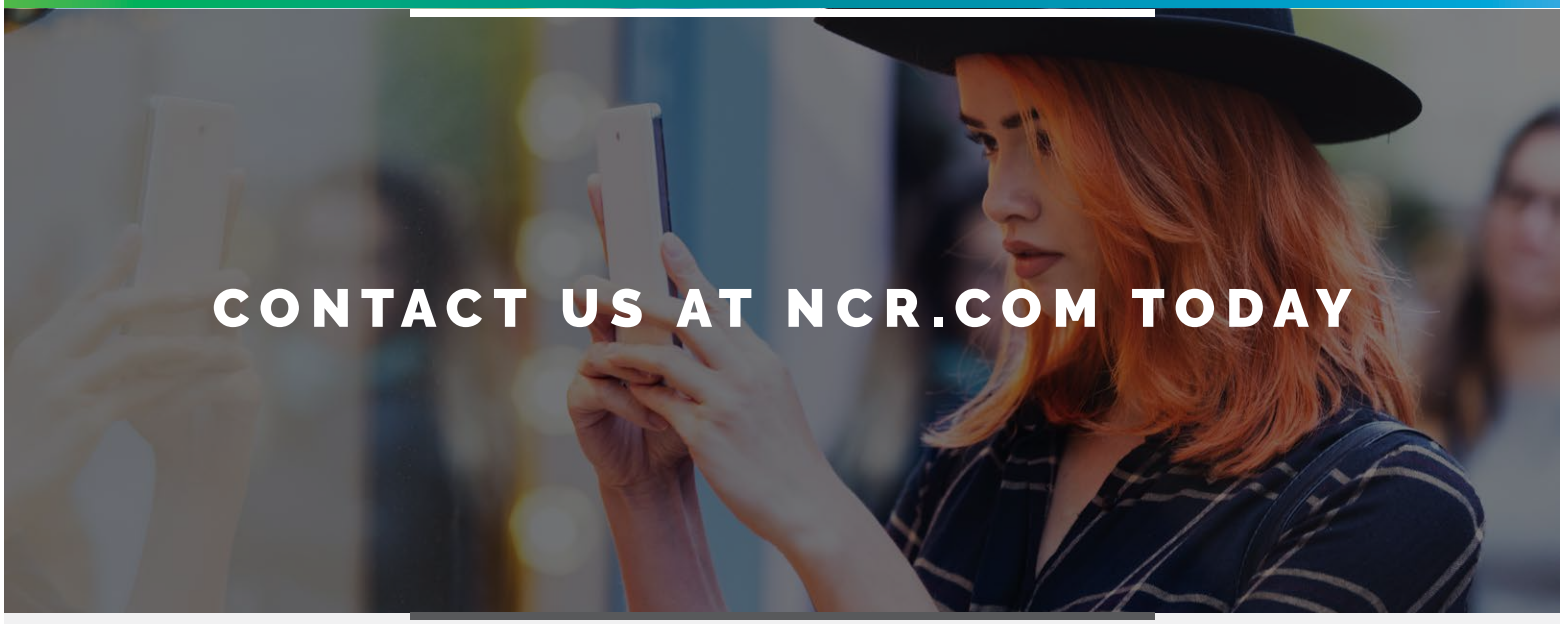
NCR Secure Pay automatically utilizes token replacement, also known as tokenization, which allows NCR Counterpoint to store a token instead of an actual card number. The card number is stored at the NCR Secure Pay host in its encrypted database. This functionality is used to store a customer's card number in a protected environment for future purposes, such as validated returns and card-on-file transactions.

Point-to-Point Encryption (P2PE)

Point-to-Point Encryption (P2PE) helps protect sensitive credit and debit card data from the first card swipe, while in transit, and all the way to the NCR Secure Pay host. State of the art encrypting devices encrypt cardholder information prior to performing an electronic payment transaction. These sophisticated devices use strong encryption and industry standard key management technologies to encrypt and transmit cardholder data securely over any network.

NCR Secure Pay provides Point-to-Point Encryption for credit and debit transactions when an encrypting MSR is used. The MSR hardware is injected with NCR Secure Pay encryption keys, so NCR Counterpoint does not have the actual card information. Only the NCR Secure Pay host has the keys to decrypt the data before sending it to the credit processor.

Completing the payment security puzzle



CONTACT US AT NCR.COM TODAY

WHY NCR?

NCR Corporation (NYSE: NCR) is a leader in omni-channel solutions, turning everyday interactions with businesses into exceptional experiences. With its software, hardware, and portfolio of services, NCR enables nearly 700 million transactions daily across retail, financial, travel, hospitality, telecom and technology, and small business. NCR solutions run the everyday transactions that make your life easier.

NCR is headquartered in Atlanta, Ga., with over 30,000 employees and does business in 180 countries. NCR is a trademark of NCR Corporation in the United States and other countries.