NorthStar

WHITE PAPER

Protecting guest card data, from tap to token.

Your network carries more than orders. It carries every card, phone and watch your guests pay with. Here is how the payment security layers fit together, what changed with PCI DSS v4, and the five network practices that keep your restaurant from becoming the weak link.

$11.5M
AVERAGE COST OF A U.S. DATA BREACH
IBM, 2026

247
DAYS, ON AVERAGE, TO FIND AND CONTAIN A BREACH
IBM, 2026

31%
OF BREACHES START WITH AN EXPLOITED VULNERABILITY
Verizon DBIR, 2026

v4.0.1
THE ONLY SUPPORTED PCI DSS VERSION
PCI SSC, 2025

INSIDE

Network Security Best Practices for Restaurant Payments

01 The security challenge
02 Follow a card through your restaurant
03 The payment security stack
04 Wallets, tap and pay at the table
05 Five network practices
06 Choosing a partner

EXECUTIVE SUMMARY

Card security is a network problem, not just a terminal problem.

Guests pay by card, phone or watch dozens of times a shift. Every one of those payments crosses your network, and every crossing is a chance for card data to leak. Malware planted on POS systems and registers has long been one of the most common ways card data gets stolen from restaurants.

There is no single fix. Protection comes in layers: PCI DSS compliance, EMV and contactless at the terminal, point-to-point encryption (P2PE) in transit and tokenization at rest. Then the everyday discipline of running a clean network. This paper walks through each layer and how they work together.

01 THE SECURITY CHALLENGE

A breach costs far more than the card numbers.

IBM's 2026 Cost of a Data Breach report puts the average U.S. breach at **$11.5 million**, more than double the global average of $4.99 million, which is itself a record.[1] Organizations took an average of **247 days** to identify and contain a breach. That is eight months of exposure.

Attackers are getting in through the gaps nobody patched. Verizon's 2026 Data Breach Investigations Report found **31% of breaches** began with an exploited vulnerability, now the top way in, and ransomware showed up in **48% of breaches**.[2]

High transaction volume, lots of hands on the system, shared networks and thin IT staff make restaurants attractive. Card data is the prize, and the POS is the path in.

WHAT A BREACH ACTUALLY COSTS

- **Forensics and recovery.** Outside investigators, cleanup and new equipment.
- **Downtime.** Terminals offline means tables you can't close.
- **Notification.** Every U.S. state has its own breach notification law, and they don't all match.[3]
- **Card brand penalties.** Fines and higher processing costs after a compromise.
- **Lost guests.** Nobody wants to wonder if their card was stolen at your table.

No magic bullet

SECURITY IS AN ONGOING FIGHT

Every layer closes one gap and leaves another open.

EMV stops counterfeit cards but does nothing after the reader. PCI DSS sets the rules but can't stop malware on its own. The answer is layers that cover for each other, so **card data is useless to anyone who steals it,** wherever they steal it.

02 FOLLOW A CARD THROUGH YOUR RESTAURANT

Four moments where card data needs protecting.

A single payment touches the reader, your POS, your network and the processor in a couple of seconds. Each layer of security guards a different stretch of that trip.

STEP 1 · READER

Tap, dip or wallet

The chip or phone creates a one-time code for this payment only.

EMV & CONTACTLESS

STEP 2 · AT THE READ

Encrypted instantly

Card data is scrambled inside the reader, before your POS or network ever sees it.

P2PE

STEP 3 · IN TRANSIT

Across your network

Only the processor can decrypt it. Anyone listening in gets noise.

P2PE

STEP 4 · AT REST

Stored as a token

Your system keeps a random stand-in for tabs and refunds, never the real card number.

TOKENIZATION

PCI DSS The rulebook that covers every step above, plus the people, passwords and processes around it.

03 THE PAYMENT SECURITY STACK

What each layer does, and what it doesn't.

THE RULES

PCI DSS

The Payment Card Industry Data Security Standard applies to any business that stores, processes or transmits card data. Version 4.0.1 is now the only supported version, and the requirements introduced in v4.0 became mandatory on March 31, 2025.[4] Compliance is the floor, not the ceiling.

AT THE TERMINAL

EMV and contactless

Chip cards and contactless taps generate unique data for every transaction, so stolen data can't be replayed to build a counterfeit card. The catch: EMV authenticates the card. It doesn't protect the data once it leaves the reader.

IN TRANSIT

Point-to-point encryption

P2PE encrypts card data the moment it's read and keeps it encrypted until it reaches the processor. Your POS and network never handle a readable card number, and a validated P2PE solution can shrink how much of your environment falls in PCI scope.

AT REST

Tokenization

Tokenization swaps the card number for a random value that's worthless outside the payment system. Tabs, refunds and repeat charges run on the token, so there is no card number sitting in your system to steal.

> Most operators land on a hybrid: P2PE to protect data in motion, tokenization to protect it at rest.

04 WALLETS, TAP AND PAY AT THE TABLE

Faster checkout turned out to be safer checkout.

Mobile wallets like Apple Pay, Google Pay and Samsung Pay are built on tokenization. The phone never hands over the real card number, and each payment is approved on the device with a face, fingerprint or passcode.

For restaurants, that means shorter lines at the counter and less card data exposed at every step. Pay at the table and handheld devices bring the same protection to full service. **When the card never leaves the guest's hand, it never leaves their sight.**

HOW NORTHSTAR HANDLES IT

NorthStar Order Entry protects card data with tokenization and supports point-to-point encryption, so card data is secured from the moment it's read. EMV, contactless and mobile wallet payments run on the same platform, at the counter, the kiosk and the table.

05 FIVE NETWORK PRACTICES

Encryption is the start. Your network is the rest.

The technology above protects the card. These five habits protect everything around it: the network, the devices and the people with access.

01

Keep a hardened firewall

It is your first line of defense, and PCI DSS requires network security controls. Back it with anti-malware and keep it current.

02

Patch everything, promptly

POS software, operating systems, routers and apps. Updates close the holes attackers already know about, and the median time to patch a known exploited flaw is now 43 days.[2]

03

Control who gets in

Give staff and vendors only the access they need. Keep payment systems off guest Wi-Fi. Use unique logins, strong passwords and multi-factor authentication. Never leave default passwords in place, and lock down remote access.

04

Scan and assess regularly

Run vulnerability scans, know every device on your network and check for new risks before someone else finds them.

05

Train your team

Most attacks start with a person: a phishing email, a shared password, a USB stick. Teach every employee your policies and why they matter.

PLAN FOR THE BAD DAY

Protecting against a breach matters. So does limiting the damage if one happens.

Cyber insurance. Many carriers offer coverage built for data breach exposures. Know what yours covers before you need it.

A response plan. Decide now who you call first, who talks to guests and how you keep taking payments while systems are checked.

06 CHOOSING A PARTNER

Attackers keep moving. Your partner has to move faster.

Network attacks and data breaches aren't going away. Criminals keep finding new angles, and the standards keep changing to meet them. Keeping up takes a partner who understands restaurant payments end to end.

Look for a track record in restaurants and the know-how to match the right protection to your operation, whether that's a single location, a growing franchise or an enterprise with hundreds of stores.

Questions to ask your POS provider

- **Is card data encrypted at the reader,** before it touches the POS?
- **Do you tokenize stored card data** for tabs, refunds and repeat charges?
- **Do you support EMV, contactless and mobile wallets** on every device?
- **How do you ship security updates,** and who installs them?
- **How do you help with PCI DSS** and keep my scope small?
- **Who picks up the phone** when something looks wrong?

SOURCES

1. IBM, *Cost of a Data Breach Report 2026* (breaches from March 2025 to February 2026), published July 30, 2026, via Baker Donelson and Security Boulevard.
2. Verizon, *2026 Data Breach Investigations Report* (incidents from November 2024 to October 2025), via CyberScoop, 2026.
3. National Conference of State Legislatures, Security Breach Notification Laws.
4. PCI Security Standards Council, PCI DSS v4.0.1, the current version. v4.0 retired December 31, 2024; future-dated requirements effective March 31, 2025.

NorthStar

TALK TO OUR TEAM

Secure payments, built into the POS.

CBS NorthStar is a restaurant POS and order-management platform built for QSR and full-service operators: iPad-based Order Entry POS, payments, kiosk, customer-facing display, loyalty integrations and third-party delivery on one platform, backed by hands-on rollout and support since 1994.

(800) 551-7674 · info@cbsnorthstar.com · cbsnorthstar.com

#findyournorthstar