

# 10 Strategies for Android mPoS Security

PCI Compliance for Mobile Point-of-Sale

# 10 Strategies for Android mPoS Security

- Understand Shared Responsibility 2
- Understand PCI Obligations 3
  - Understand Applicable Frameworks 3
  - Understand PCI Compliance Guidelines 4
  - Maintaining Compliance 5
- Lock mPoS Against Unauthorized Use 5
- Deploy P2PE or Tokenization 6
- Actively Manage mPoS Health 7
- Monitor for Tampering 8
- Manage Network Security 9
- Centralize Your Asset Management 9
- Be Proactive About Updates 10
- Work with an Expert 11



These days, many leaders in customer-facing industries are switching to mobile point-of-sale (PoS or mPoS) - and for good reasons!

- Traditional PoS solutions are heavy and clunky.
- Many employers find that it's hard to train new employees on outdated PoS systems.
- Most traditional PoS systems rely on the vendor for security updates, which can happen sporadically or never.
- Traditional point-of-sale repairs and upgrades require on-site technician visits, which can cost thousands of dollars annually.

It's easy to see why the total cost of ownership for traditional PoS is much higher than mPoS when you factor in training, repair, and security risks.

Switching to mPoS can be an opportunity to improve your organization's PoS compliance, especially if you're proactive about total device health.

Business technology leaders face a lot of pressure to automate their retail point-of-sale operations and discover cost efficiencies. While switching from traditional PoS to Android mPoS makes clear sense for most organizations, you'll likely be called upon to prove these efficiencies.

In this whitepaper, you'll learn how the scope of your PCI responsibility and security obligations for Android mPoS stacks up to your traditional PoS obligations, and how to proactively manage an Android mPoS deployment for 24/7 compliance.

*Please note that Esper.io is NOT a qualified security assessor (QSA) for your PCI DSS obligation. Similarly, we are not a substitute for qualified legal council. Instead, we're a leading option for Android mPoS migration. Any guidance in this whitepaper is designed as an overview and should be carefully vetted by a qualified compliance advisor.*

# 10 Strategies for mPoS Compliance

1

## Understand Shared Responsibility

The [Payment Card Industry Data Security Standard](#) (PCI DSS) is a set of bare minimum security and compliance standards for merchants and service providers. The PCI addresses both traditional and mobile PoS, along with card readers, networks, routers, servers, online shopping carts, and paper files - plus operational controls for people and processes at organizations like your own.

Shared responsibility is a crucial configuration for retailers who are looking at the possibility of configuring, monitoring, and maintaining any type of point-of-sale device - including both traditional mobile point-of-sale or An-

droid mPoS. Typically, retailers share their PCI responsibility with vendors such as Esper.

The full scope of your shared responsibility may not be completely clear during a traditional mPOS deployment. In these cases, it can be difficult to estimate your responsibility around IT staff, system resources, or secure network bandwidth -- especially as a system ages and requires updates. With an Android mPoS deployment, it can be much easier to estimate your long-term IT, system, and network requirements.

## Understand PCI Obligations

While it's essential to consider PCI compliance at the beginning of a mPoS modernization project, it's also entirely possible to control, segment, and treat PCI compliance risks when switching to mPoS.

It's important to note that mPoS does not necessarily create compliance risk.

It just changes existing compliance risks and removes some of the problems associated with traditional point-of-sale. Android mPOS has plenty of unique PCI DSS requirements, but it can diminish your burden to update traditional PoS machines or perform updates on-site.

### • **Understand Applicable Frameworks**

Once again, your organization and your compliance and legal counsel bear the responsibility to understand all federal, state, and regional requirements for payment security and privacy.

These frameworks can vary significantly depending on where you operate. However, they may include the Payment Card Industry Data Security Standard (PCI DSS), PCI-related state legislation (Nevada, Washington, and Minnesota), and The European Union Privacy Directive.

Ask a Qualified Security Assessor (QSA) or legal council for additional details.

PCI compliance standards mandate minimum standards for how merchants and other businesses handle credit card information securely, which helps diminish the chances that cardholders data is breached or compromised. If merchants don't process credit card information under PCI Standards, the card data could be hacked and used in a variety of fraudulent actions.

## • Understand PCI Compliance Guidelines

Being PCI compliant means always adhering to a set of guidelines set forth by the PCI Standards Council. PCI compliance follows standards by the PCI Standards Council, an organization formed in 2006 to manage cardholder data security security.

The requirements developed by the Council are known as the Payment Card Industry Data Security Standards (PCI DSS). PCI DSS has six significant objectives, 12 essential needs, 78 base requirements, and over 400 test procedures.

**The guidelines are also considered security best practices. Its six critical requirements include the following:**



Build and maintain a secure network and systems



Protect cardholder data



Maintain a vulnerability management program



Implement strong access control measures



Regularly monitor and test networks



Maintain an information security policy

## • Maintaining Compliance

All companies which process credit card information must continue PCI compliance - as directed by the agreements they have with their card processors. PCI compliance is considered an industry standard. Businesses that are not compliant can face substantial fines due to

agreement violations and negligence. Companies that are non-compliant are also highly vulnerable to fraud, theft, and data breaches -- including immensely costly clean-up fees and regulatory fines, plus a long-lasting loss of customer trust.

### 3

## Lock mPoS Against Unauthorized Use

While there are many advantages to switching to mPoS, don't underestimate the risks of employees or customers who attempt to misappropriate mPoS devices for their personal use.

Personal use may not always be nefarious in intent, but it can still create risks. Some examples of usage that's not entirely malicious but is still a security risk could include an employee who downloads insecure apps from the Play Store or a random website to a mobile point-of-sale tablet. Even if the employee didn't intend to compromise security

or compliance, they could still compromise the integrity of your cardholder data environment on the mPoS device.

To keep things safe, you should lock mPoS against all forms of unauthorized use and avoid dual-use cases that increase the amount of personal and payment data on a single device. For example, avoid using a self-service payment kiosk for use cases related to your loyalty program or employee time-keeping apps.

It's crucial to lock devices to single-app Android kiosk mode where the payment app is locked to full screen and users cannot exit it. Effective solutions will prevent employee attempts to factory reset the device.

Also, it's best to create controls against kiosk mode by setting your payment app to load to full-screen mode from the moment a device boots up (or, is powered on). Mobile payment apps should

load to full-screen mode at the same time you start the device.

Esper specializes in locking Android mPoS apps to unbreakable full-screen, single-app kiosk mode. We make it easy and fast for our customers to remotely lock point-of-sale apps to full-screen mode and maintain these configurations remotely.

## 4

### Deploy P2PE or Tokenization

Using a PCI-validated source for either point-to-point encryption (P2PE) or tokenization can reduce the scope of your PCI responsibility significantly. In these cases, the tokenization or P2PE vendor will maintain most of the responsibility to protect cardholder data.

P2PE and Tokenization operate similarly to reduce your scope of PCI responsibility. The only communication

between processor/card capture and the mPoS device is to provide an anonymized token. This token shows whether payments were accepted or declined without providing any data that's considered in-scope for PCI DSS - the tokenization or P2PE vendor is responsible for protecting cardholder data.



## Actively Manage mPoS Health

Payment infrastructure is complex under any conditions (regardless of whether you're using mPoS or traditional PoS). Stores may have PoS terminals, self-check units, kiosks, or other hardware connected to app pro-

viders and back-office servers, a network, enterprise mobility management solutions (EMM), and numerous other vendors and components.

**Treating PCI compliance risks involves actively monitoring the total state of device health including:**



Operating system



Applications



Configurations



Content files



Users



Device

At Esper, we lead the industry with solutions for visibility and control over all the above device state of health factors, so you can actively manage each of these components in real-time.

Android mPoS offers a visibility advantage over traditional mPoS systems,

which are not typically integrated with a backend for active management. You can achieve a more active security and compliance posture by switching to mPoS to proactively address any issues with your PCI DSS requirements year-round.

# 6

## Monitor for Tampering

Tampering can be an attempted misappropriation of mPoS for innocent personal use, such as a bored employee who tries to download TikTok during quiet hours at work. It also would include a hacker's attempt to steal cardholder data for financial gain by trying to modify the apps, firmware, hardware, or other components of a point-of-sale system.

Esper helps organizations monitor unauthorized apps, configuration changes, and telemetry data that shows whether a device is unplugged, broken, has a low battery or used in ways that show tampering, such as settings modification. This type of visibility is generally not provided with traditional point-of-sale systems.

With traditional PoS systems, retailers are typically forced to rely on in-store employees to report any suspicious behavior or tampering attempts.

mPoS is not always mobile. It can be tied down to location with various hardware that makes it impossible to move. mPoS can also be mobile for table-side service. Regardless, Esper can also geofence mPoS or track location to see when a device has been stolen and create an automated device lock. Esper can be configured to automatically lock or "brick" an Android mPoS & device if it's ever moved off-site.

### Esper helps organizations monitor



## 7

### Manage Network Security

P2PE or tokenization reduces the scope of PCI network security obligations and risks since the processor is responsible for encrypting the data. That means the company that owns and uses the mPoS device doesn't have to worry about data transmission security over their network. However, network security is still critically important.

mPoS modernization provides an enormously important opportunity to find and treat existing network security risks. It would help if you had all mPoS devices

on a unique network. Don't use the same network used for other retail devices, such as computers, tablets, or kiosks that are used for non-payment use cases. Network segregation is a crucial control against network-related threats.

We can't emphasize this enough, never use open public WiFi that customers can access. Regardless of your encryption method and whether you're using traditional or Android mPoS, you are responsible for making sure that your network is secure.

## 8

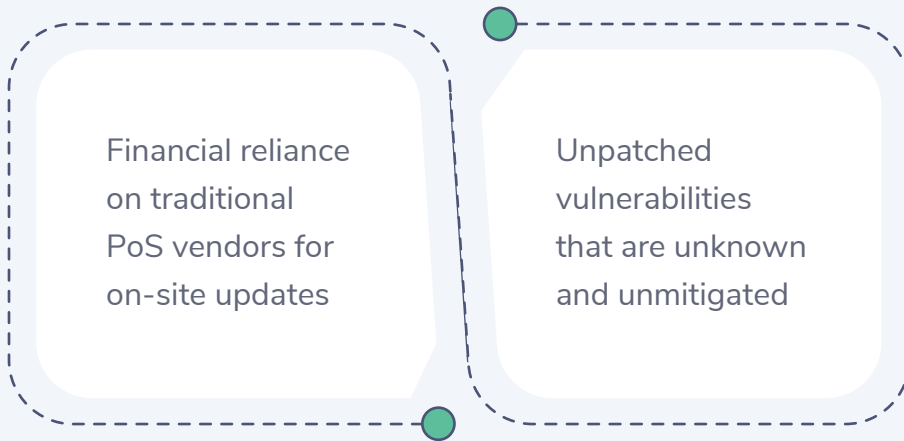
### Centralize Your Asset Management

Proper device management is critical. mPoS are mission-critical devices since they generate revenue, and you must manage them accordingly. Ideally, they should be a part of a more significant initiative toward creating full visibility

into all remote assets, including visibility into non-payment tablets, kiosks, and network devices.

Many organizations lack a centralized way to track their traditional PoS. They can't log in and see a list of remote devices--including which ones are

working and which need updates. In a traditional point-of-sale model, this can create the following issues for retailers:



Esper offers organizations the ability to monitor and manage mPoS and other remote Android devices so organizations can reduce risks long before their audit.

## 9

### **Be Proactive About Updates**

Unpatched vulnerabilities are an enormous security risk source in any circumstance - including mPoS, traditional PoS, kiosks, and everything else. It's essential to think about updates to mPoS holistically. Even if the P2PE/tokenization vendor manages payment capture and transmission, the device still needs to be

updated quickly and frequently to a healthy state.

Make sure you keep your PoS apps, operating system, and configurations updated to avoid vulnerabilities that could compromise your customer's cardholder data.

Esper can simplify the complex process of device protection by offering managed services for mPoS apps and configurations. This includes Android firmware updates to Esper's custom Android operating system, Esper Enhanced



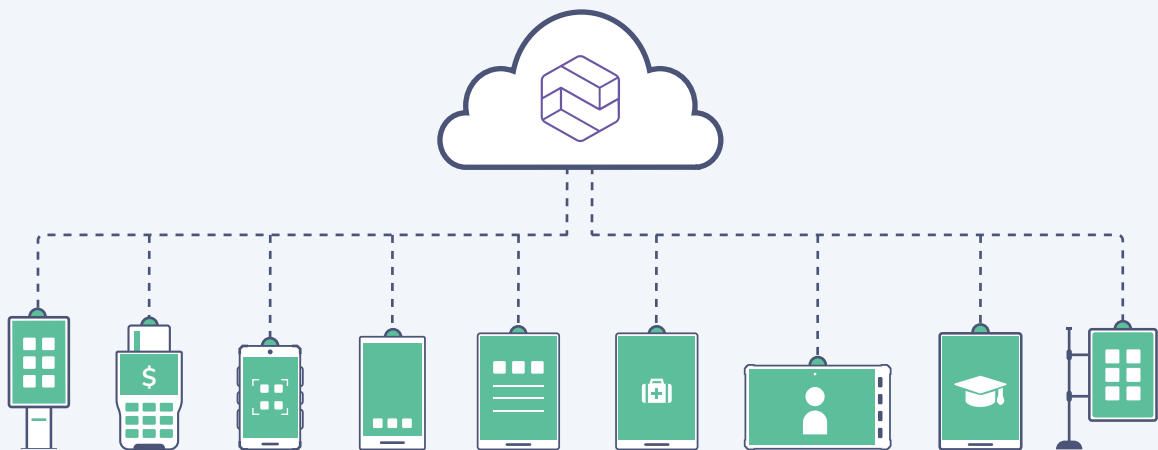
Android (EEA) to reduce the burden of applying patches on your own.

# 10

## Work with an Expert


Esper helps our customers with many of the aspects of mPoS systems, including customers in the retail sector who are household names for quick service restaurants and hospitality. We connect Android devices to the cloud, including mobile point-of-sale systems, kiosks, employee tablets, student tablets, and healthcare devices.

Esper is not an Android mPoS compliance vendor. We also don't claim to be a substitute for a qualified security assessor (QSA), which is why we encourage our customers to seek expert guidance on PCI compliance. However, we can help our customers switch to Android mPOS and assume shared responsibility for some PCI DSS requirements.





## PCI DSS Responsibility for Android mPoS


### Requirement 1: Install and Maintain a Firewall to Protect Cardholder Data

| Customer  | Esper | Notes   |
|---|-------|---|
|  |       | You are responsible for maintaining all network firewalls at your retail point-of-sale location with traditional OR mobile point-of-sale. |

### Requirement 2: Change All Vendor-Supplied Defaults


| Customer  | Esper   | Notes   |
|---|---|---|
|  |  | Customers use Esper to remotely create and maintain secure mPoS configurations. |

### Requirement 3: Protect stored cardholder data



| Customer  | Esper | Notes   |
|---|-------|---|
|  |       | Esper's partners for P2PE and tokenization can help you reduce the scope of your cardholder data protection requirements. |





#### Requirement 4: Encrypt transmission of cardholder data across open, public networks

| Customer  | Esper | Notes   |
|---|-------|---|
|  |       | Esper's partners for P2PE and tokenization can help you reduce the scope of your cardholder data transmission requirements. |



#### Requirement 5: Use and regularly update anti-virus software or programs

| Customer  | Esper   | Notes   |
|---|---|---|
|  |  | Esper's managed firmware over-the-air updates can streamline your operating system update requirements. |



#### Requirement 6: Develop and maintain secure systems and applications

| Customer  | Esper   | Notes   |
|---|---|---|
|  |  | Esper can help you maintain greater lifecycle visibility and control over your mPoS devices, apps, and configurations - especially compared to traditional point-of-sale! |



### Requirement 7: Restrict access to cardholder data by business need to know

| Customer  | Esper   | Notes  |
|---|---|--|
|  |  | Esper can help you lock your Android mPoS against unauthorized access and track health in real-time. |

### Requirement 8: Assign a Unique ID to each person with access

| Customer  | Esper   | Notes  |
|---|---|--|
|  |  | Esper can help you create secure admin, employee, and customer access roles for your Android mPoS. |

### Requirement 9: Restrict physical access to cardholder data

| Customer  | Esper   | Notes   |
|---|---|---|
|  |  | Esper is one of the only solutions to provide real-time insight into mPoS location, battery, and other signals of device health and security. |



### Requirement 10: Track and monitor all access to network resources and cardholder data

Customer

Esper

Notes



Use Esper to create audit logs of on-site and administrative users.

### Requirement 11: Regularly test secure systems and processes

Customer

Esper

Notes



Esper's DevOps pipelines allow you to roll config, firmware, app, and other updates forward and back.

### Requirement 12: Maintain a policy that addresses info security for all personnel

Customer

Esper

Notes



Turn policy into practice with Esper's user-friendly provisioning templates for Android mPoS.

Contact Esper to learn more about rapid mPoS modernization and how an intelligent switch to Android mPos can streamline your PCI compliance by providing visibility, control, and remediation at each stage of the device lifecycle.

[Click here to book a demo](#)

OR

email us at  
[andi@esper.io](mailto:andi@esper.io)



esper.io