

# What's New For SAQs

# Lauren Holloway

Director, Data Security Standards

# John Bloomfield

Manager, Data Security Standards

PCI Security Standards Council



# What's New for PCI DSS v4.0 SAQs?



# General Changes for all SAQs

Response*			
<i>(Check one response for each requirement)</i>			
In Place	In Place with CCW	Not Applicable	Not In Place
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

# E-commerce Methods

E-commerce Method	SAQ Type for Eligible Merchants	How many PCI DSS v4.0 Requirements
Merchant has no access to own website	<b>SAQ A</b> <b>Fully Outsourced</b>	11
Merchant website redirects customers to a compliant TPSP (e.g., URL redirect)		27
Merchant website includes a compliant TPSP's embedded payment page/form (e.g., iframe)		29

# E-commerce Methods

E-commerce Method	SAQ Type for Eligible Merchants	How many PCI DSS v4.0 Requirements
<p>Merchant has no access to own website. Merchant website creates the payment form, and payment data is delivered directly from the consumer browser to the TPSP (often called a “Direct Post”)</p>	<p><b>SAQ A-EP</b> <b>Fully Outsourced</b></p>	11
<p>Merchant website includes a compliant TPSP’s embedded payment page/form (for example, an iframe). Merchant website loads or delivers a script(s) that runs in the consumer browser (for example, JavaScript)</p>		27
	<p><b>Except for the Payment Page</b></p>	139
		29

All other e-commerce methods and implementations

**SAQ D for Merchants**

**All PCI DSS Requirements**

# SAQ A – Why New Requirements?

- Many SAQ A merchant breaches...
- Requirement for ASV scanning & FAQ 1485
- New v4.0 requirements for payment page protection

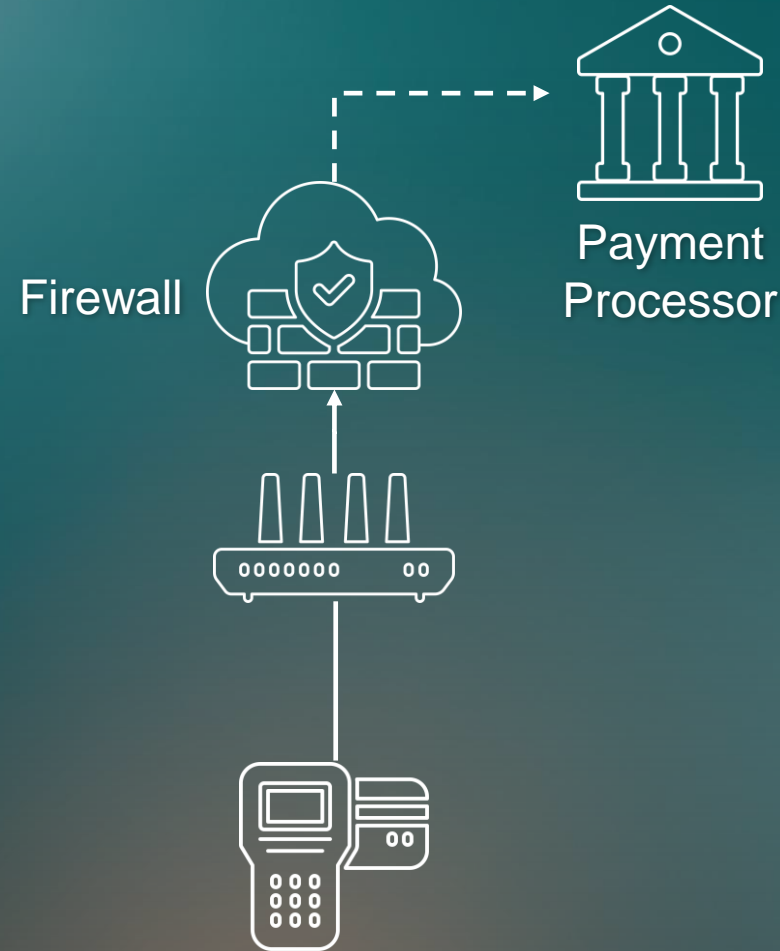
# SAQ B-IP

---

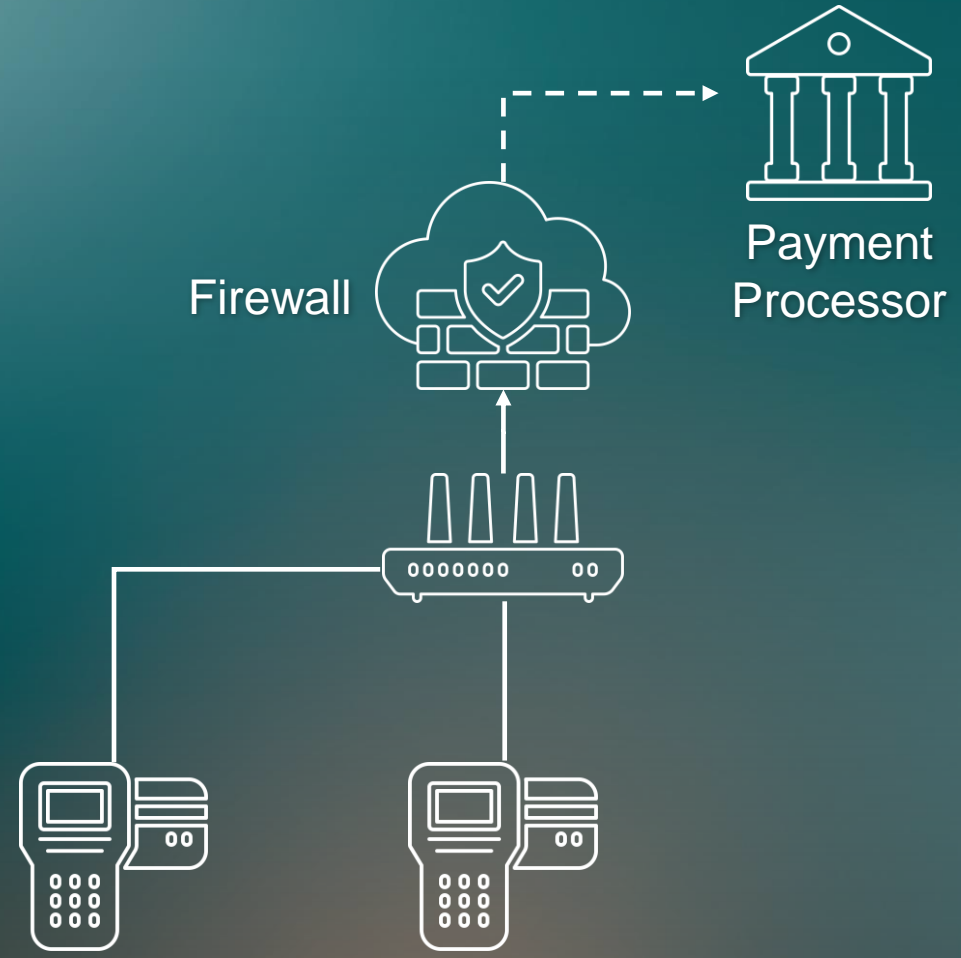
For approved PIN Transaction Security (PTS) Point-of-Interaction (POI) devices

What does “devices are not connected” mean?

# Connections Eligible for SAQ B-IP

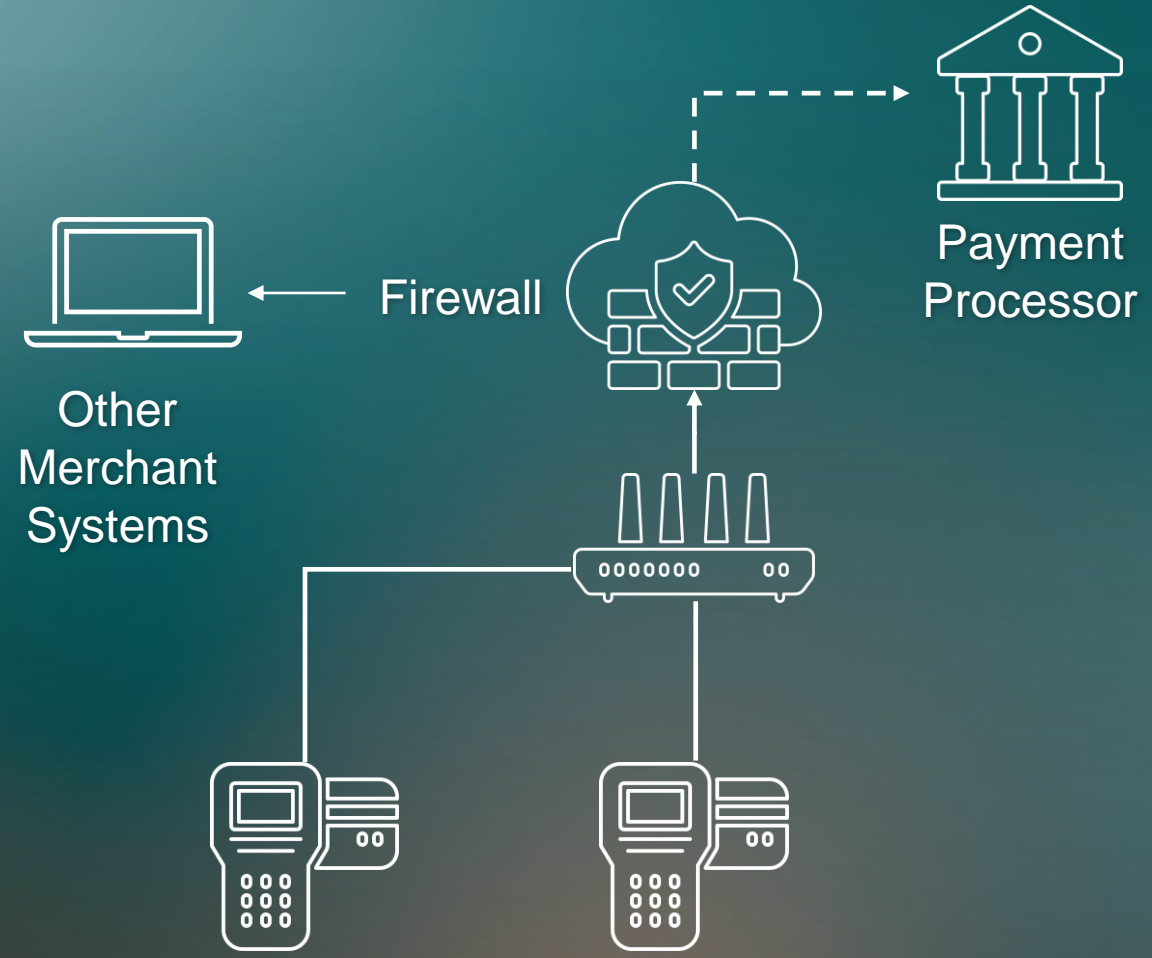


# Connections Eligible for SAQ B-IP



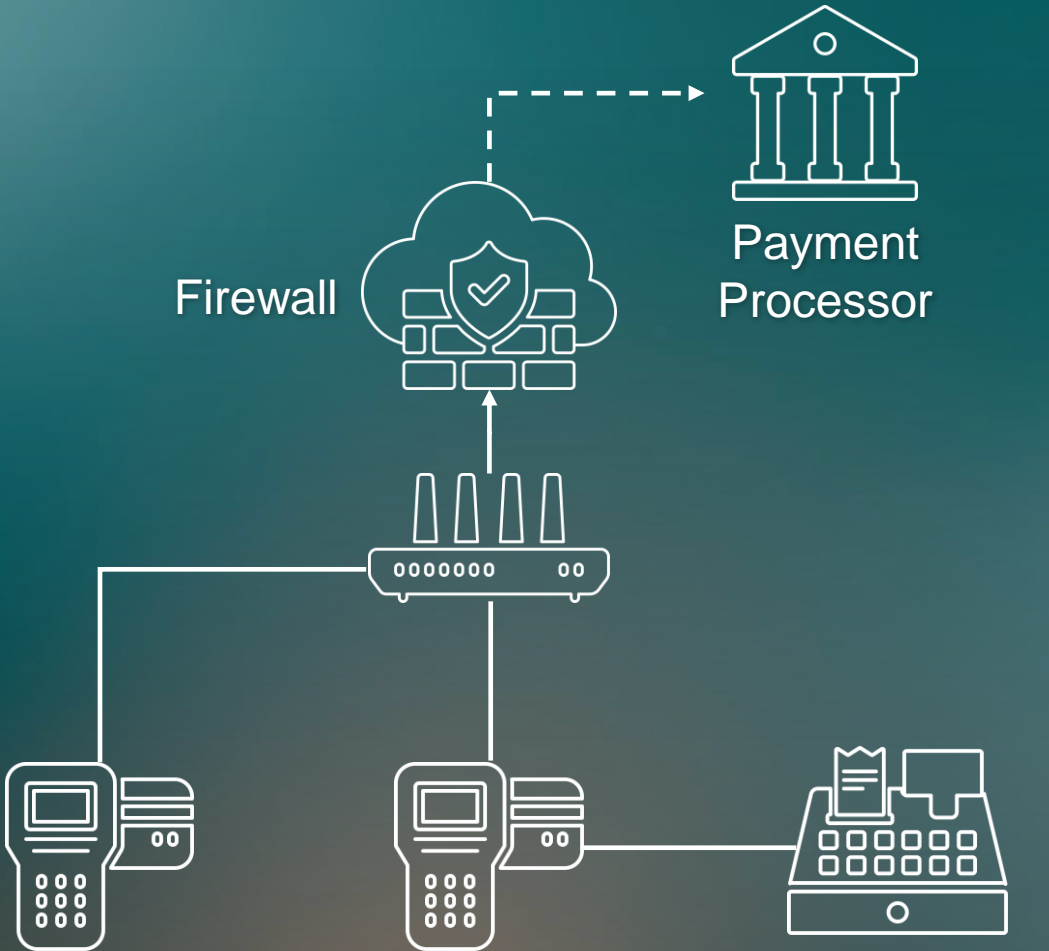
Multiple IP-connected PTS-approved POI devices in same network zone

# Connections Eligible for SAQ B-IP



Multiple IP-connected PTS-approved POI devices in same network zone

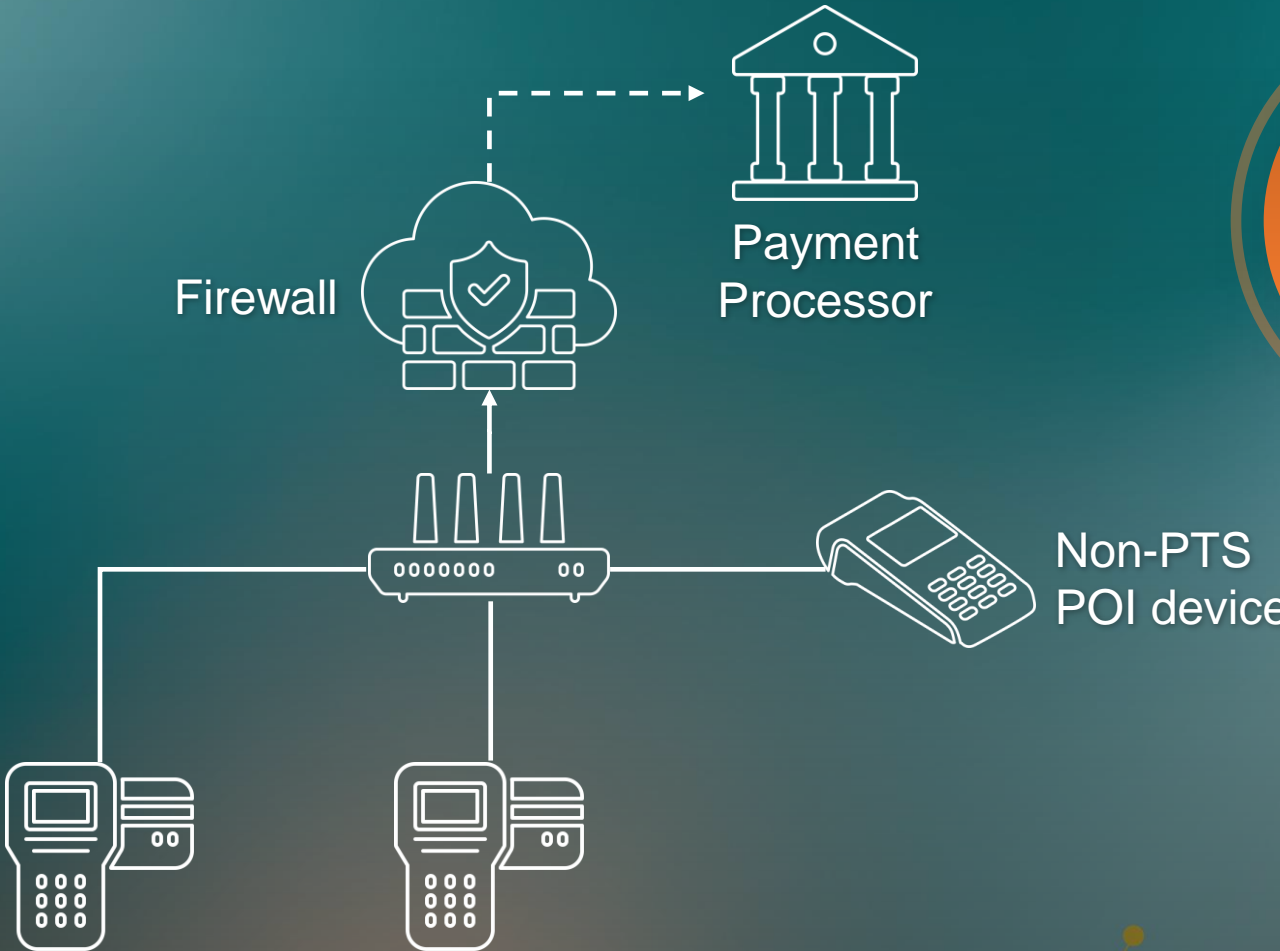
# Connections **Not** Eligible for SAQ B-IP



Multiple IP-connected PTS-approved POI devices in same network zone

Cash Register

# Connections **Not** Eligible for SAQ B-IP



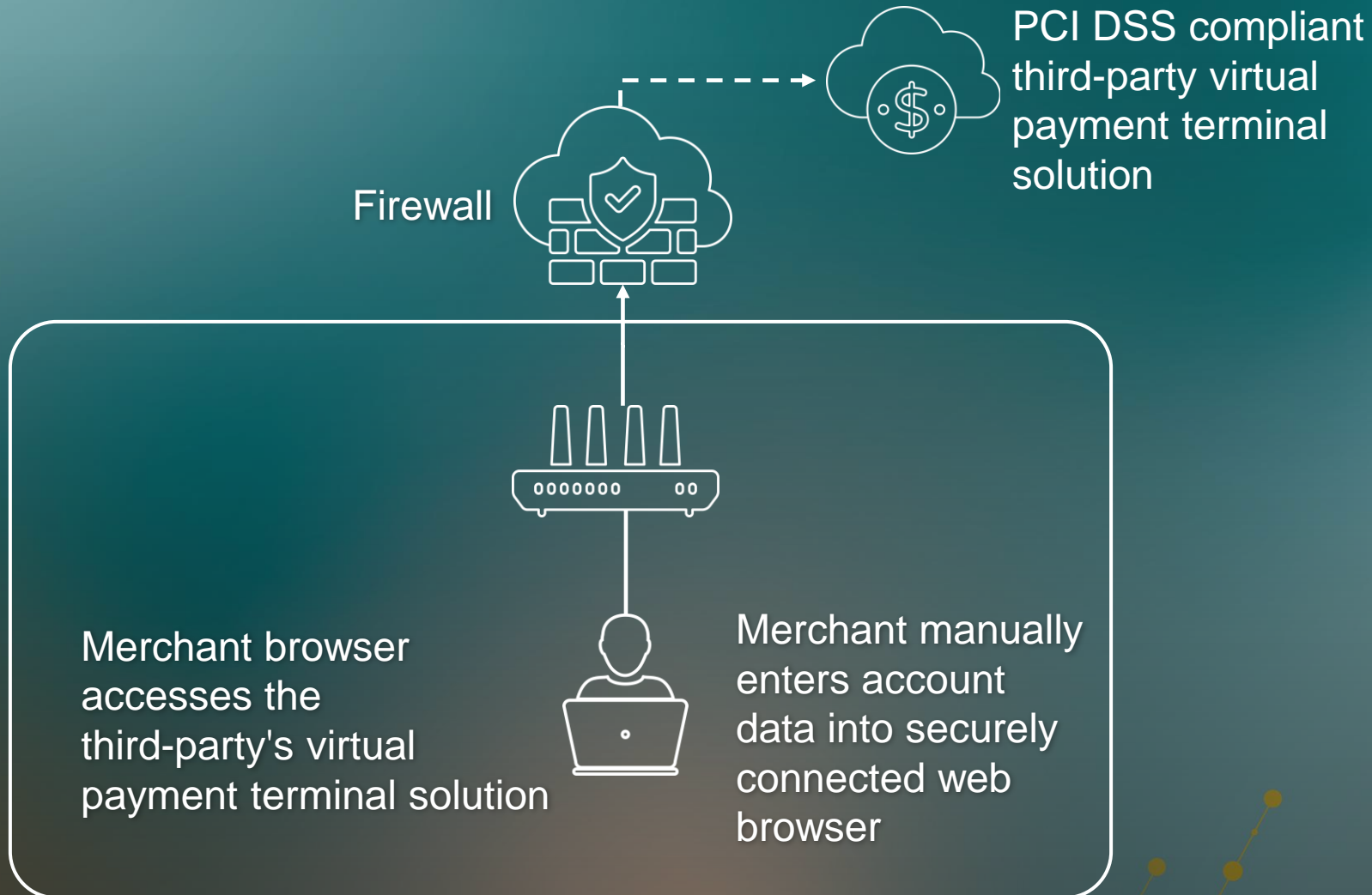
Multiple IP-connected PTS-approved POI devices in same network zone

# SAQ C-VT

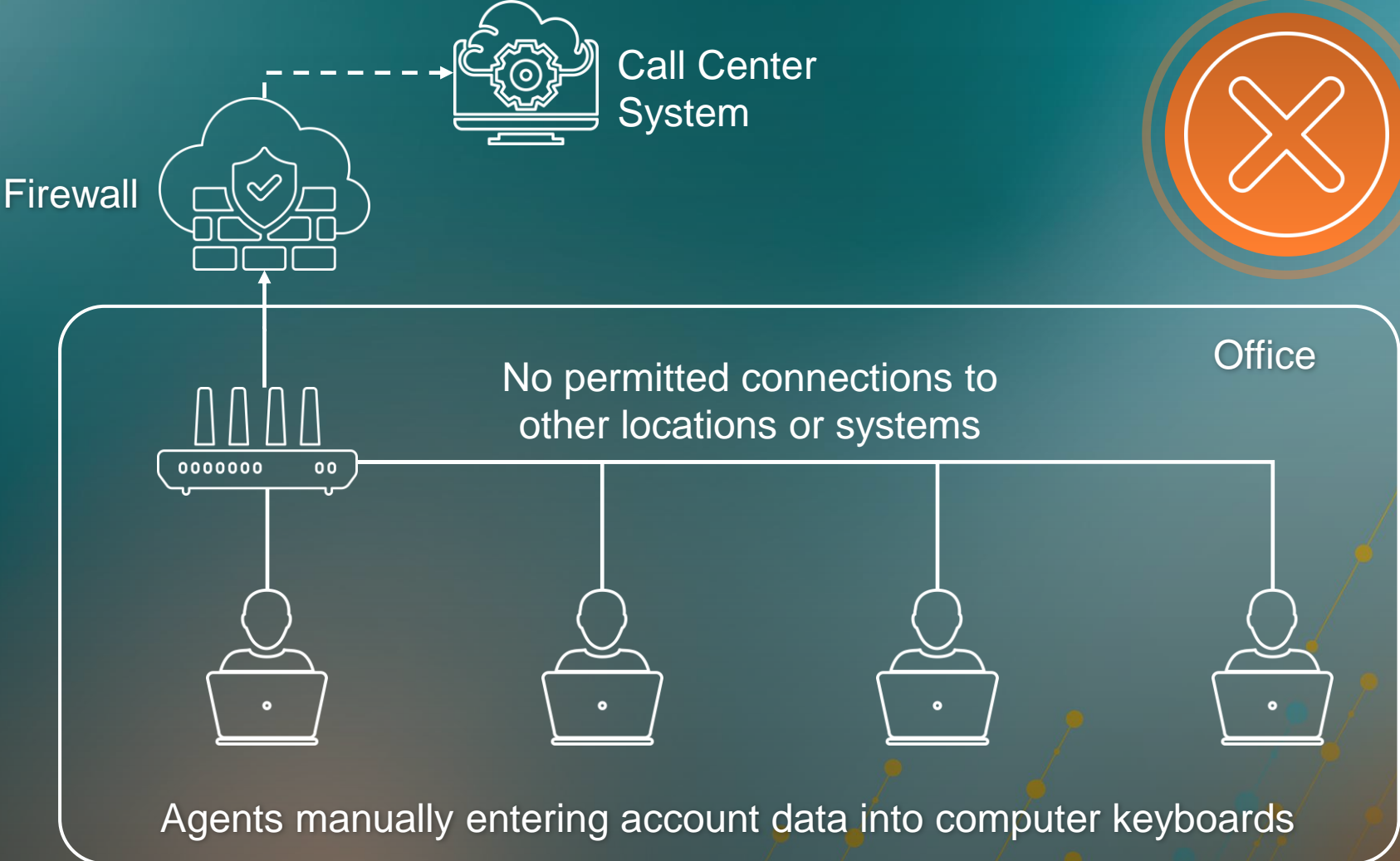
---

What does “no connections to other locations or systems” mean?

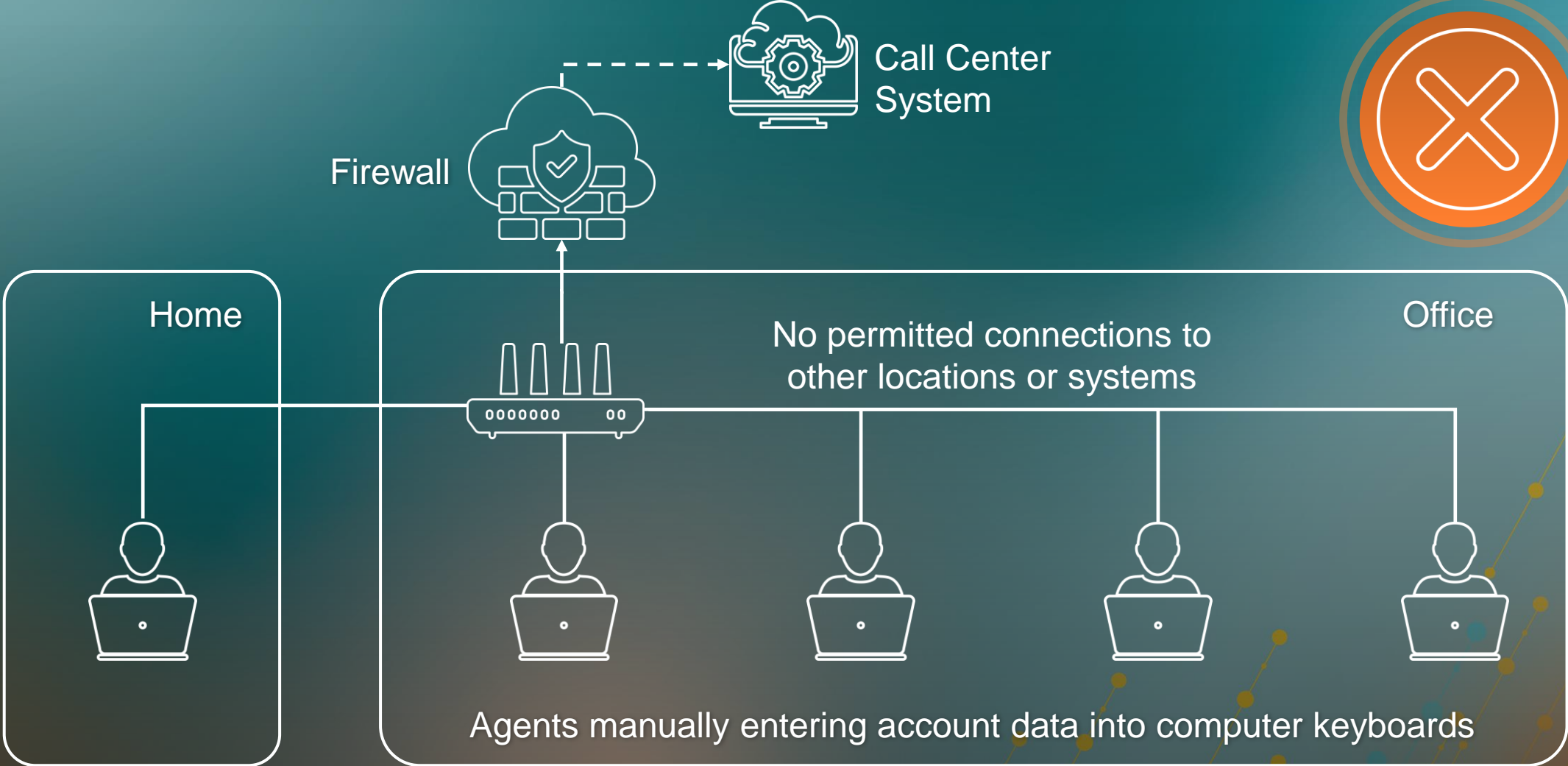
# Connections Eligible for SAQ C-VT



# Connections **Not** Eligible for SAQ C-VT



# Connections **Not** Eligible for SAQ C-VT



# Things That Don't Exist...



SAQ A  
for  
Service  
Providers

# SAQ D for Service Providers

- The only SAQ for Service Providers
- Statement added to all SAQs

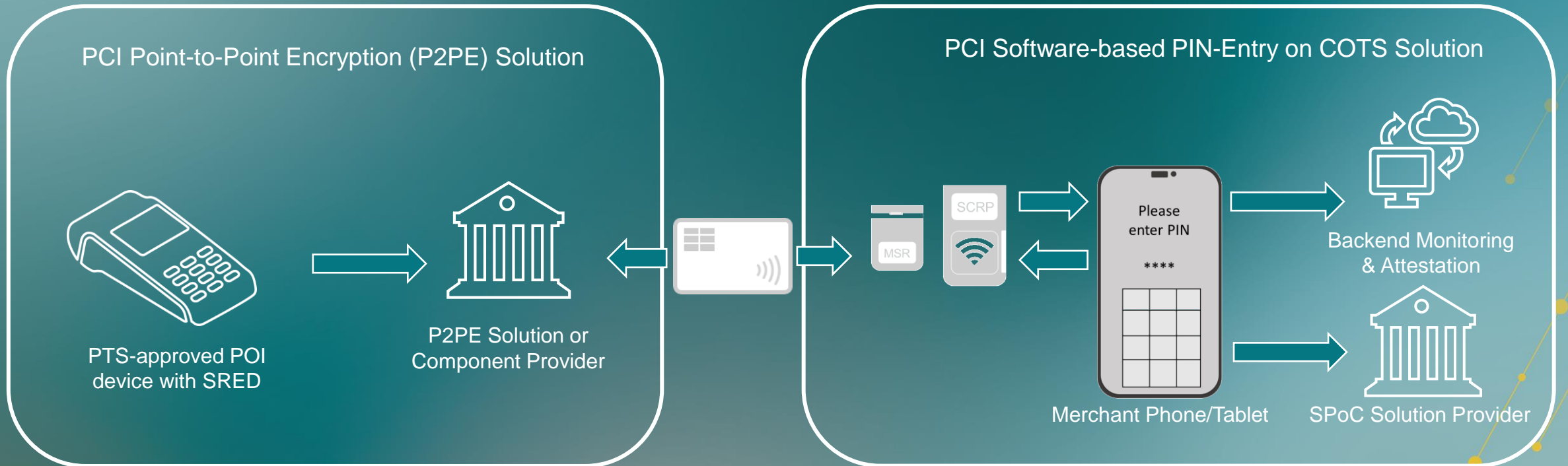
# What Changed in SAQ D for Service Providers?

- Higher expectations for entities that provide services on behalf of others
- Additional documentation requirements in v4.0



# SAQ Instructions and Guidelines v4.0 and a New SAQ

# Difference Between P2PE and SPoC



PCI P2PE protects payment account data via encryption from the point it is captured in the merchant's payment device until it is decrypted in a P2PE solution or component provider's environment.

PCI SPoC facilitates mobile payment acceptance solutions that enable secure transactions with PIN on a merchant's commercial off-the-shelf (COTS) device (phone or tablet).

# Future SAQs?

**Thank You!**