PCI Compliance Support from McKesson

Are you ready for the September 17, 2013 Bank of America directive?



Credit card providers have required that Bank of America (BoA) Merchant Services obtain proof of compliance with the Payment Card Industry Data Security Standard (PCI DSS) from its customers. BoA notified 2,000+ McKesson pharmacies that they must provide BoA with proof of PCI compliance by September 17, 2013.

McKesson anticipated this action and has provided tools and support to make achieving this deadline easier. Services are provided by McKesson's PCI and Security partner, ANX. Fully achieving PCI compliance can be time consuming and difficult for a pharmacy owner. So whether you need a little help or a lot, know that McKesson is committed to helping you meet the BoA deadline while reducing the risk of a costly data breach.

	Features	McKesson PCI Protection Plan	Secure Cloud Gateway Option
PCI Protection	\$100,000 Data Breach Protection Services	✓	
	PCI Self-Assessment Questionnaire (SAQ) wizard with task management and reporting	✓	
	PCI eLearning courses (versions for cashier, IT, and owner)	✓	
	Security Policy Templates	✓	
	ASV External Vulnerability Scanning	\checkmark	
Security	Secure Cloud Gateway (SCG) managed stateful inspection firewall with 24 x 7 monitoring, and optional WiFi support		✓
	Unified Threat Management (UTM)/ anti-malware, intrusion detection, and web content filtering		✓
	Secure remote access with two-factor authentication		✓
	Automatically answers up to 50% of the PCI SAQ		✓
Pricing		All pharmacies enrolled in a McKesson POS program are already covered at \$25 per month	\$85 per month (add \$10 for WiFi) Remote Install = \$250 Professional Onsite Install = \$375

Want More Help?

Let the PCI experts at ANX guide you through compliance with our PCI Compliance Assistance Services

- Guided PCI SAQ completion
- Guided setup of required employee eLearning
- Guided creation of PCI DSS approved security policy
- One-time ASV Scanning (if required)
- Remediation assistance to obtain a passing ASV scan (if required)
- Guided completion of the Attestation of Compliance (AOC)

249 for SAQ-B \$499 for SAQ-C*

*Available with purchase of optional Secure Cloud Gateway

18 Steps to PCI Compliance

Using the Portal

☐ Get to Know the Portal

- □ **Step 1:** Review the Portal training videos on www.McKessonPCI.com.
- □ **Step 2:** Log into the Portal:

https://mckesson.trupci.com

- Username: your MID (As written on the Bank of America letter, including the dash.)
- Password: ch@ngeme2 (You will need to change your password once you log in.)

□ Policies and Security Training

- □ Step 3: Using the Manage tab -> Manage Account of the Portal, load all employees as users into the Portal.
- □ **Step 4:** Identify which employees interact with customers/ handle credit cards/cash registers.
- □ **Step 5:** Using the Manage tab -> Manage Account, assign the employees identified in step 4 to the "Cashier's PCI Training" course.
- □ **Step 6:** Using the Manage tab -> Manage Account, assign the remaining employees to "Security Awareness" course.
- □ **Step 7:** Using the Home page -> create an information security policy (company AND employee policies) using the provided template (left column).
- □ **Step 8:** Using the Learn tab -> Manage Policies, assign the information security policies to all employees.
 - Assign policies to any new employees who are hired in the next year.
 - Update and re-assign policies annually.

□ Complete a Compliant Self-Assessment Questionnaire

□ **Step 9:** Using the Assess tab -> SAQ, click Add New.

□ Step 10: Click Help me determine which SAQ and pre-fill the SAQ. (The wizard will determine which SAQ is appropriate for your pharmacy.)

Note: Your SAQ must be both 100% complete AND 100% compliant to meet the Bank of America requirements.

☐ If SAQ B:

- □ **Step 11:** Still in the Assess tab, continue with the SAQ Wizard to complete the 29 questions truthfully.
- □ **Step 12:** Identify remediation tasks for any "no" responses.
- □ Step 13: Include explanations and evidence for any "compensating controls" or "not applicable" responses.
- □ **Step 14:** Complete remediation tasks or write remediation plan.
- □ Step 15: Continue to step 17, below.

☐ If SAQ C or D:

- □ Step 11: Still in the Assess tab, continue with the SAQ Wizard to complete the 80 (SAQ C) or 280 (SAQ D) questions truthfully.
- □ **Step 12:** Identify any remediation tasks for any "no" responses.
- □ Step 13: Include explanations and evidence for any "compensating controls" or "not applicable" responses.
- □ **Step 14:** Complete remediation tasks or write remediation plan.
- □ Step 15: Identify the IP address and type (static or dynamic) for your firewall.
- □ **Step 16:** Using the Scan tab, run an external vulnerability scan using the Portal.
 - a. Validate that the scan is "passing" according to PCI DSS guidelines.
 - b. If the scan fails, take the necessary steps to remediate each of the failures.

Please note: If the scan fails, you have the option of purchasing the Secure Cloud Gateway option from McKesson to meet PCI DSS requirements.

□ Validate Compliance

- □ **Step 17:** File and Submit SAQ and Attestation of Compliance (AOC).
- □ **Step 18:** Notify ANX (through the Portal) that your compliance materials are ready for verification.

You have the option of purchasing the PCI Compliance Assistance Services from McKesson to walk you through each of these steps required to meet the PCI DSS requirements. Please see reverse side for details and pricing. Contact us below to sign up today before the September 17, 2013 deadline.