Monthly PCI DSS Checklist

Please use the following checklist as a reminder to keep card data security a top priority for protecting your customers and your business. This is just one of many tools intended to support you in your PCI Compliance Validation efforts. In some cases, references are made within these documents to other PCI Validation Support Tools, the entire set of which can be found here at www.paymentstart.com/secure.

ALL BUSINESSES		YES	NO
1	**Did you hire any new employees this month?**		
	If so, were they trained on PCI DSS?		
	If they have access to your card data environment, were they assigned unique passwords?		
	Was the user role assigned to this new employee the appropriate level of access for your business's card data environment?		
2	**Did employees with access to your cardholder data environment leave your organization?**		
	If so, did you remove their access to your cardholder data environment?		
3	**Was any new equipment added into your card data processing environment? If so,**		
	Did you update your inventory check list?		
	Did you update your point of sales (POS) environment diagram?		
	Did you update your profile in the PCI Compliance Manager and revalidate, if necessary?		
4	**Have you completed a monthly physical inspection of your POS environment (a POS Evaluation form has been provided for your convenience)?**		
5	**If you use physical security controls (cameras, locks, etc.), have you performed a visual/physical inspection of those devices to ensure all are accounted for, that no unknown devices are found, and that they are working appropriately?**		
6	**Are you destroying all media (paper or electronic records) that contain credit card data in an approved fashion?**		
7	**Have any of your security procedures changed? If so, have you updated your security policy accordingly?**		

Elavon

	BUSINESSES PROCESSING VIA INTERNET CONNECTION	YES	NO
1	Have you reviewed all of your firewall and router configurations and rule sets?		
2	Have you changed the passwords in your environment lately?		
	If so, does the password meet the PCI DSS requirements, such as using alpha and numeric characters as well as using capitalization and special characters? In addition, recent passwords should not be reused.		

	BUSINESSES USING INTERNET CONNECTIONS AND HAVE OTHER PRODUCTS ATTACHED TO THE ENVIRONMENT	YES	NO
1	Have all system patches been deployed/updated accordingly?		
2	Is your anti-virus turned on and up to date?		
3	Have you checked all the data ports/phone jacks in your environment to ensure that no strange or unknown devices have been installed?		
4	Have all audit reports and file ‘logs’ been reviewed to ensure that no unknown network traffic has entered your environment? (This is recommended daily, especially for larger businesses.)		
5	Have you documented all changes to your security controls?		
6	Have you completed your required quarterly vulnerability scans and/or penetration tests?		

This document is intended to support, summarize, and implement data security best practices and does not replace or supercede the Elavon Terms of Service, Merchant Operating Guide, the PCI DSS standards, payment card network rules and regulations, or the Elavon PCI compliance program, as may be amended from time to time. The materials and recommendations herein are general in nature and may not apply to all merchant payment configurations or to unique data security diagrams.

Elavon