Surviving the PCI Audit Job Aid

Virginia Department of Motor Vehicles: Workforce Development Division

Use this job aid to review the PCI questions with your coworkers. Take turns asking each other questions so you can be prepared for the upcoming PCI audit.

Section I: Your PCI Role

Question	Answer
What do you do for DMV?	**Example for employee who does not handle credit card payments:** 1. I work at a work location at DMV Headquarters that does not handle payment card data or payment card information. 2. I would call the PCI hotline number for further instructions.
How do you deal with payment card data? 	**Example for employee who handles credit card payments with the card being not present.** 1. I work at a work center at DMV Headquarters that handles payment card data; however, the card is not present. 2. I enter payment data into our payment processing system according to policy. **Example for employee who handles credit card payments with the card present:** 1. I work at a CSC that handles payment card data. 2. The customer retains their card and authorizes the payment by swiping or inserting their card into the card reader. I then process the payment according to policy.

Section II: PCI Training

Have all staff been trained on PCI procedures? Can you describe some of the training?	All staff has been trained on PCI procedures through the mandatory eLearning. And, employees that handle credit card payments have had additional PCI training.
How frequently does PCI training occur?	PCI training is required annually and during onboarding for new hires.
Where do you find PCI policies and procedures for your work location?	Agency PCI policies and procedures are located on the myDMV intranet.

Section III: Information Security

Question	Answer
Have you and your staff been trained to verify the identity of third-party maintenance personnel who come to "repair" your payment card machines?	Our PCI eLearning covers this. Since DMV doesn't contract with outside companies to fix our credit card machines, we would report the approach of third-party maintenance personnel to our manager.
Are you aware of authentication policy and do you follow it? For example, do you use strong passwords to protect authentication credentials?	Yes, we are each assigned a unique ID for computer access. Our systems are all password-protected using strong passwords. VITA won't let us create a weak password.
Are shared or generic credentials used in your work center?	Logons and passwords are not shared. Every employee has a unique ID in our systems.
Have you been trained to report suspicious behavior or indications of device tampering on your payment card machines?	Yes. All employees are required to take a PCI elearning that covers what to do about device tampering and suspicious individuals.
Have you completed security awareness training and are you aware of the importance of cardholder data security?	Yes. We are required to take annual IT Security Awareness training that covers PCI security, as well.
Have you been trained on incident response procedures if you suspect a data breach? For example, your computer screen looks like it is being controlled remotely – such as your mouse moving on its own or you see a suspicious pop-up.	Yes. DMV's annual IT Security Awareness training, required for all employees, instructs us to stop using the computer and immediately contact our Information Security and Risk Management Office, or call the PCI Hotline if we suspect a data breach.
What do you do if you receive a suspicious email?	We forward it to the Information Security and Risk Management Office and delete it from our system without clicking on any links it may contain.

Section IV: Credit Card Machines

What procedures are used to inspect credit card machines?	Our managers periodically inspect the machine to look for tampering. However, we must also be aware of suspicious behavior around the credit card machines.
Do you have procedures to follow if a credit card machine needs to be replaced or repaired?	Yes, we would notify our manager. Employees do not install, replace, or return credit card machines.
What has STAFF been instructed to do in the event that they suspect credit card machine tampering?	We must report suspicious behavior and indications of credit card machine tampering to our manager or DMV's Information Security and Risk Management Office.
What do MANAGERS do if staff reports suspicious incidents regarding credit card machines?	Our manager would report suspicious incidents to DMV's Information Security and Risk Management Office. If our manager is unavailable, we may call the PCI hotline.

Section V: Authorization

How is authorization to process payment cards revoked if it is no longer needed for your job function?	The manager collects all the equipment such as badges, key FOBs, and phones. HR and IT by are notified by completing an SAR13 form to shut off system access.
How do you regularly monitor and test the controls over cardholder data?	Managers do it through daily observations by observing computer monitors, credit card machines, daily reconciliations, and audits.
Do you understand the security policy for restricting access to cardholder data?	Yes. I have taken the eLearning training on DMV's IT Security policy. We restrict access to cardholder data both physically and electronically on a need-to-know basis.
How is access to restricted areas authorized so that physical security is maintained over cardholder data?	Our work center is restricted to DMV employees only with access badges visible at all times.
Are all visitors authorized and escorted in areas where cardholder data is processed or maintained?	Yes. If visitors are in the work center, they must be pre-authorized by the manager and escorted at all times. In addition, since cardholder data is susceptible to unauthorized viewing, copying, or scanning, it is not left unprotected while on someone's desk or in a stack of filing.

Section VI: Improper Channels for Out-of-Scope Locations

Question	Answer
What are the proper or authorized channels for receiving cardholder data?	There are methods that protect cardholder data such as in person, by fax, or on the phone.
What are improper channels for receiving cardholder data?	DMV does not accept cardholder data through email, postal mail, or voicemail.
Is cardholder data stored?	Only if there is a compelling business reason.
For in-scope, card present locations, what do you do to safeguard the payment card data?	For locations that regularly process payment cards, we refer to our individual administration's procedures for specific instructions.

Section VII: Improper Channels for In-scope Locations - Card-Present or Card-Not-Present Locations

What do you do if you receive payment card information through an improper channel?	In my position, I do not process credit card payments. So I would call the PCI Hotline and have them walk me through the process.
Does your area have any deviations from the proper/improper channel process?	No. Only if there is a compelling business reason would we do anything different.
What procedures are used to destroy hard-copy cardholder data?	If written down, the credit card number is shredded immediately to prevent fraudulent use.
Describe the work flow that is followed by your in-scope location when a customer's payment card information is received through an improper channel.	If we receive customer payment card information through an improper channel, there are several things that we must do. Each work center must follow their appropriate procedures. DMV will enter the cardholder's information (not the card number) into an improper channel log. DMV will send the customer a letter saying we no longer accept payment card information through improper channels.
But, what about postal mail?	For **postal mail**: The document containing the customer's payment card information must be shredded.
And for email?	For **email**: The customer's email must be deleted from both the mailbox and the deleted items folder.
What would you do if you received a Full-PAN through voice mail?	For **voice mail**: The customer's voice mail must be deleted from the phone.