PCI Breach Reporting Article no. 4708

Resolution Steps

PCI Breach Reporting

Employees are our first line of defense in protecting customer information.

For this reason it is important for all of us to know the process for reporting PCI violations. If you personally see, or suspect any type of data breach, you should immediately contact your supervisor/manager. If your supervisor/manager is not available, escalate it up to the next available manager. The supervisor/manager will contact the local Human Resources leader.

Examples of a breach include, witnessing an employee copying down credit card information on paper and hiding it in a purse or backpack or using a camera to take photos of a computer screen, etc. You receive a call for a customer who states they believe their credit card information has been stolen from an employee, etc. Also it is important to be aware of any visitor or contract personnel looking in or around areas, where customer information can be found.

Another type of breach may on your computer equipment. If you suspect that any software has been attached to your computer through an external source, immediately stop using your computer and alert your supervisor/manager and your local IT representative. Just to further emphasize, do not wait until your supervisor/manager is available, report it up to the next level of management; quick action is how we will protect our customer information.

If you have any questions regarding our PCI Policy or how to report a breach, please contact your supervisor who will reach out to their local HR Leader.

Online URL: https://agentx-astound-kb-qa.hgsdigital.com/article.php?id=333