WAM OnPoint Scan Data Sharing Program Data Integrity and Security

WHAT WILL MY DATA BE USED FOR AND WHERE WILL IT GO?

Data integrity is one of our core values. Your data will only be used in an anonymized and aggregated format (meaning it does not contain any store-level information) for things like identifying opportunities, negotiating better programs and promotions (with current and prospective OnPoint and WAM manufacturers), and to provide you with recommendations to improve sales, except as noted below.

Your data will be shared with your WAM distributor so they can provide you with reports and insights (including, but not limited to, Customer Business Reviews) to help you better manage your business.

If you participate in OnPoint Promotions, your store-level transaction data will be provided to participating manufacturers to validate promotional results and payments.

WHAT DATA DOES THE SOFTWARE COLLECT AND WHERE IS THE DATA STORED?

The Transaction Collector software collects your scanned UPC sales movement data from your POS electronic receipt journal, which is essentially the same as the paper receipts you hand out to a customer when a transaction is complete.

No personal or payment information is collected about the customer as your POS already masks this information in the electronic journal files before we can retrieve them. This is mandated by PCI compliance federal law.

Your data, once collected, is sent to our secure servers via a secure web API where it is stored.

WHERE IS THE TRANSACTION COLLECTOR SOFTWARE INSTALLED AND HOW DOES IT INTERACT WITH MY POS?

The Transaction Collector software program is a Microsoft Windows based program that is installed on your back-office computer that is networked to your POS.

Your back-office computer is networked to your POS via your Payment firewall MNSP (Managed Network Service Provider). You may recognize the firewall unit from names like Mako, Cybera, SageNet, Hughes, Paysafe, Fortinet, Acumera, etc. Your MNSP is who helps to monitor your payment services and makes sure you are in PCI compliance with your equipment that is connected to the payment firewall. You should not need to action any whitelist provisioning for this software with your MNSP.

If your location utilizes an internal firewall or antivirus program managed by you or your company and you need to whitelist the program so it will work, we can provide that information on request.

If your POS utilizes a username and password that the Transaction Collector needs to access to retrieve the files, the software stores that information in an encrypted file on your PC, as well as updating the password every 30 days.

412.246.8800
contact@onpointds.com