

DynaFlex II Go products are PCI PTS v6.x SCR, certified. The packaging is designed to be tamper evident and the closure uses security tape. Any attempt to open the package shows signs of tampering. This document explains how to detect tampering.

### Overall Form Factor

The basic form factor of the package is a folded white cardboard box with a cardboard insert where the device is nestled into Korrvu plastic wrap packaging. There are no rips or added materials on the package other than product and Lot labels. The package only has one color ink printed on the package: black. The box is made with corrugated white cardboard.

#### BACK OF PACKAGE

##### Certification Compliance Logos

Industry certification logos showing compliance are printed on the back of the package as shown. Manufacturer address is shown.



#### FRONT COVER OF PACKAGE

The front cover of the package lists the product name, MagneSafe Security information, PCI revision information, product read capability icons, QR Codes, and description.



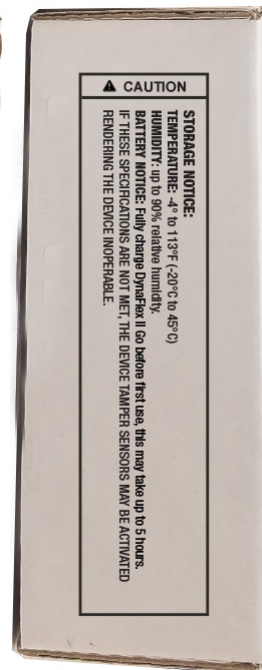
#### LEFT SIDE OF PACKAGE

On the left side of the package is printed a list of the package contents and the product label is adhered.



#### RIGHT SIDE OF PACKAGE

The right side of the package shows the storage requirements and CAUTION content.



#### FRONT OF PACKAGE

The front of the package lists the product name, category, PCI certification, and Security Tape.



**Adhered**  
Here security tape is applied and secured. Wrapping front to bottom of package.



**Tape - Removed Tape**  
Tape is removed VOID and OPENED appear on tape.



**Package - Removed Tape**  
Tape is removed VOID and OPENED show as the inverse ink on the package.

#### SECURITY TAPE

Security tape wraps onto the bottom of the package from the front flap of the package.

## ADDITIONAL DETAILS AND CHECKLIST

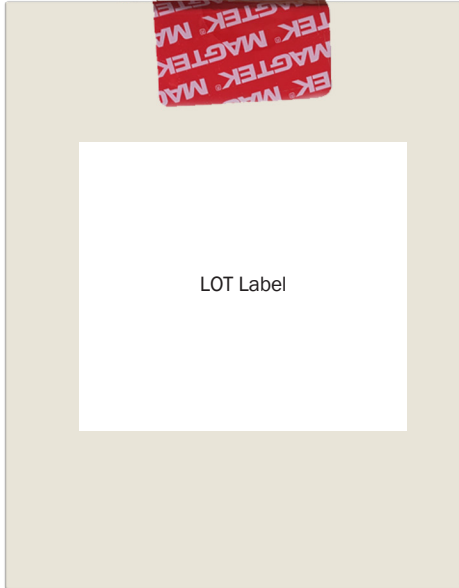
**BOTTOM**

**Security Tape**

The Security Tape wraps from the front flap to the bottom of the package. Make certain there are no signs of tampering.

**Lot Label**

The Lot label is placed on the bottom of the box. Make certain there are no false labels added or tampering.



**PCI DEVICE VALIDATION**

To check for PCI Validation check the Hardware and Firmware ID. Hardware ID is printed on the label. The Firmware ID is accessible via the device. Go to the PCI compliance web page and search for MagTek, and find the product name, DynaFlex II Go. Compare the Hardware ID and Firmware ID: [https://www.pcisecuritystandards.org/assessors\\_and\\_solutions/pin\\_transaction\\_devices](https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices)

As part of your inspection, include the following for your device inspection audit:

- Be certain to have a list of the devices and include the details listed on the product label.
- It may be helpful to take photos of the front, back, and sides of each device.

Be certain to check device part numbers, serial numbers, and IDs and check physical connections. Use the chart below as a checklist to inspect the device for signs of tampering.

Are there signs of tampering:	Signs of tampering	
	YES	NO
<b>Package Inspection</b>		
Form Factor - check overall form factor		
<b>Front</b>		
Check form factor		
Look for signs of tamper		
Check printing and no added labels		
<b>Left, Right, and Back Sides</b>		
Check form factor		
Look for signs of tamper		
Check printing and no added labels		
Check product label		
<b>Front Flap</b>		
Check Security Tape		
Look for signs of tamper		
Check printing and no added labels		
Check form factor		
<b>Bottom</b>		
Check Security Tape		
Look for signs of tamper		
Check printing		
Check form factor		
Check lot Label		

**INSIDE**

DynaFlex II Go products are nestled inside the package with Korrvu packaging that uses cling wrap to hold the device securely in place for transit. The cling wrap is attached to an insert that has thumb-hole cuts on either side to make it easier to remove from the outer packaging. The package includes the device, cable(s), device inspection document, and quick installation guide.



**NOTICE:** Follow RMA procedures. User should report all signs of tampering as per standard protocol.