[DATE]

As a longstanding trusted advisor in the industry, HID is committed to proactively assessing the needs of our customers and outlining recommended best practices. This blog outlines a recent issue uncovered by HID. We become aware of the unauthorized use of third-party parasitic devices designed to harvest power or communication from a host HID reader ("unauthorized devices"). The use of an unauthorized device with an HID reader is an improper modification and misuse of the HID reader and the HID products used in conjunction with the reader. Such unauthorized devices include, but are not limited to, those listed below.

Unauthorized Devices

Safetrust, Inc.	**Proxy, Inc.**	**Suprema, Inc.**	**Zerv**
Sabre Module	Nano Connect	Airfob	Zerver A
Sabre Decal	Nano Inline		Zerver B
Sabre Cover			Zerver C
Sabre Inline			

HID does not endorse or support these unauthorized devices for use with genuine HID readers despite any claims by these manufacturers of interoperability or compatibility. We undertake extensive testing with all elements of our solutions to ensure they are safe, reliable, and durable. HID has no assurance that similar testing has been undertaken by any unauthorized device manufacturers.

Accordingly, any use of unauthorized devices with HID readers will (1) void the lifetime warranty on those readers, and (2) void the warranty on all other HID products (e.g., credentials, controllers, etc.) used in conjunction with those readers. HID does not accept liability for any potential risk or damage these unauthorized devices may pose.

Lastly, due to the unknown technical features of these unauthorized devices, HID does not provide technical support for any readers (or associated HID products) that use such unauthorized devices.

As always, our customers' security and system performance are HID's highest priority. HID cannot stress enough the importance of procuring genuine accessories and peripherals for HID products solely from HID through HID authorized channels. Our ability to provide customers with safe and secure solutions relies on ensuring that only tested and authorized devices are supported.

We are committed to updating customers with any significant changes to unauthorized list of devices in the future.