FAQ SPOOF & LIVENESS DETECTION

What is spoofing? Is it really a problem?
Spoofing is an attack at the sensor level in which a biometric sample is replaced by an imposter's sample. Susceptibility of biometric scanners to spoof attacks is a well-documented problem.

How does Precise Biometrics' technology determine if an image is live or a spoof?
Precise Biometrics' Spoof & Liveness Detection technology exploits the differences between images of live and spoof fingerprints. These differences are identified by extracting features from fingerprint images that are each unique to live and spoof biometrics.

What sensor technologies are supported by Precise Biometrics' spoof & liveness detection software?
Our liveness detection technology utilizes only the image collected to make its determination of liveness. As such, the technology is applicable to any fingerprint scanning technology.

Capacitive scanners can't be spoofed, right?
Wrong! This is a common myth. Capacitive scanners can be fooled just as easily as other types of scanners; it simply requires one to use inherently conductive spoof materials such as gelatin, glycerin or wood glue, or to add conductive "filler" (e.g., graphite) to non-conductive spoofing materials such as silicone or paint. Our spoof lab has experience with spoofing all types of sensors, including both passive and active capacitance based scanners.

How does Precise Biometrics stay ahead of subversive spoofing techniques, and incorporate countermeasures in its spoof & liveness detection technology?
Similar to countermeasure providers in the malware and antivirus industry, we continuously attempt to recognize new and emerging spoofing tactics, and also anticipate possible future spoofing approaches. To do so, we maintain an in-house spoof lab for conducting experiments and analyses of numerous materials and devices. Moreover, we work with Clarkson University and the Center for Identification and Technology Research (CITeR), to leverage their research in liveness detection.

Are there national/international standards for liveness detection? Does the Precise Biometrics technology comply with them?
No industry standards currently exist for liveness detection, but there are liveness detection standards currently under development. The most extensive standards effort for liveness detection is being conducted by the ISO/IEC Working Draft 30107. Microsoft's Windows Hello specification also includes a component on liveness detection, (a.k.a. presentation attack detection).