Frequently Asked Questions About Biometrics for Time and Attendance

What is biometrics?

Biometrics is the practice of automatically identifying people by one or more physical characteristics. The use of biometrics in time and attendance systems makes it much more difficult for one employee to clock in or out on behalf of another (i.e. "buddy punching").

What are the different kinds of biometrics?

Hand geometry, fingerprint, voice, signature, face geometry and iris or retinal scans are all in use today. Each different type has its advantages and disadvantages, making each suitable for different types of applications. Fingerprint and hand geometry are the most commonly used types for time and attendance applications.

Are there any health concerns with the use of biometrics?

No. Biometric identification and verification systems have been in use for over 25 years, with no reported health hazards. The methods used for commercial biometric identification and verification are non-invasive and pose no health risks.

What is the difference between "biometric identification" and "biometric verification"?

Biometric identification compares a biometric "signature" to all the records stored in a database to determine if there is a match.

Because it requires comparing each existing record in the database against the new biometric characteristic, it can be slow and is usually not suitable for real-time applications such as access control or time and attendance.

You'll find biometric identification used most frequently in such applications as law enforcement — for instance, the comparison of a fingerprint from a crime scene to a database of prints collected from convicted criminals.

Biometric verification compares a newly-scanned biometric characteristic to a measurement previously collected from that same person to verify that individual's identity.

For instance, when an employee is hired, that employee's fingerprint will be enrolled into the company's biometric time and attendance system. When that employee attempts to clock in the next day, her newly-scanned fingerprint will be compared to the fingerprint scan collected when she was enrolled into the system. If there is a match, the employee's punch will be recorded.

Because of this one-to-one comparison, biometric verification systems are generally much faster than biometric identification systems. Most commercial applications of biometrics for time and attendance or access control use biometric verification.

What is a "false acceptance"? What is a "false reject"?

You will often hear biometric system vendors touting their system's low false-acceptance or false-reject rate. These refer to how accurate and reliable the system is in correctly identifying people.

For time and attendance systems, a **false acceptance** occurs when the system registers a punch from an employee even when someone else's finger or hand (or an artificial finger or hand) is offered for validation. A **false reject** happens when the system refuses to accept the employee's own fingerprint or hand as valid.

Biometric systems all strive to have rates of false acceptances and false rejects as low as possible. False acceptances may allow instances of buddy punching to "slip through the cracks." False rejects can lead to employee frustration when they aren't able to clock in and out successfully using their own hands or fingerprints.

How does fingerprint biometrics work?

When an employee is first enrolled in a fingerprint-based biometric time and attendance system, the software records a template of the employee's fingerprint and associates that template with the employee's ID number. This template measures the relationship between various points in the fingerprint.

Each time the employee attempts to clock in or out, the time and attendance software verifies that the newly scanned fingerprint matches the template originally stored for that ID number. If there is a match, the punch is recorded.

Occasionally, employees will have privacy concerns about having their fingerprint scanned. The fingerprint templates used for biometric verification such as with **ATRx Secure PunchIn** are stored in encrypted format and cannot be used to re-create anyone's fingerprint. Additionally, because biometric verification uses relatively few points of comparison, the templates used in commercial time and attendance systems are useless without another fingerprint with which to compare them. They cannot be used for biometric identification.

What are the advantages of fingerprint biometrics?

Fingerprint biometric readers are generally lower cost and are often used for entry-level systems such as Acroprint's **ATRx Secure PunchIn**. They represent an easy and affordable way for businesses to get started using biometric-enabled time and attendance systems. Depending on the system, fingerprint-based biometric systems can have a false-acceptance rate that is lower than other technologies.

How does hand geometry work?

When an employee is first enrolled in a hand-geometry-based biometric time and attendance system, the hand reader records a 3-D image of the hand. The image is stored as a template associated with that employee's ID number.

Each time the employee attempts to clock in or out, the hand reader verifies that the newly scanned hand image matches the template originally stored for that employee ID number. If there is a match, the punch is recorded.

The scanners used by Acroprint's **ATRx Biometric 1000** system are highly accurate, taking 90 different measurements of the hand. The scanners also update the template every time the

employee's hand is successfully scanned. This means that the system can accommodate changes such as natural aging, weight gain, weight loss and other normal variations in the hand geometry.

Artificial fingernails and small adhesive bandages are not usually a problem. If worn consistently, jewelry such as wedding bands will likewise normally not affect the accuracy of the scan.

Some employees have hygiene concerns about placing their hand on the reader. Generally speaking, there is no greater health risk involved in using the hand reader than there would be in using a doorknob that has been touched by other people, handling money, or shaking hands. When necessary, the HandPunch reader can be easily cleaned with glass cleaner and a soft cloth.

What are the advantages of hand geometry biometrics?

Hand geometry has been in use longer than any other biometric technology, starting with the use of 2-dimensional devices in the 1970s. HandPunch systems from Acroprint such as the **ATRx Biometric 1000** use an advanced 3-dimensional hand reader for highly accurate results. In most cases, hand geometry systems will have a lower false reject rate than fingerprint systems.

This resource has been brought to you by Acroprint Time Recorder Company. Operating since 1969 with headquarters in Raleigh, North Carolina, Acroprint Time Recorder Company is a leading global manufacturer and distributor of time and attendance products with thousands of dealers and distributors across the United States and products that are exported to 70 foreign countries.

Acroprint Time Recorder Company
5640 Departure Drive
Raleigh, NC 27616
1-800-334-7190 or 1-919-872-5800
www.acroprint.com