TEAM Software
by WORKWAVE

# Who's Really on the Clock?

How Facial Verification Stops Time Theft,
Protects Your Margins and Strengthens Client Trust

TABLE OF CONTENTS



INTRODUCTION

# THE QUIET DRAIN ON YOUR PROFITABILITY

Time theft rarely looks like theft. It looks like a quick favor between coworkers — one employee clocking in for a friend who's running late, someone punching out a colleague who slipped off early. No alarms sound. No one files a report. But across hundreds of shifts and dozens of sites, those small moments add up to real money that comes straight out of your margins.

For security and cleaning companies, this challenge is amplified. Your workforce is spread across multiple locations, supervision is limited, and installing dedicated time-tracking hardware at every site is impractical and expensive. The result is a system built on trust, with little verification behind it.

Biometric timekeeping changes that equation. This guide covers what the problem truly costs, what separates a strong solution from a weak one and how WinTeam Mobile delivers facial verification without disrupting the way your teams already work.

Time theft affects an estimated
**2–5% of total annual payroll.**

For a company with $1,000,000 in annual payroll,
**that's $20,000 to $50,000**

# LOST EVERY SINGLE YEAR.

CHAPTER 1

# UNDERSTANDING THE HIDDEN COST OF BUDDY PUNCHING

Buddy punching — one employee clocking in or out for a colleague who isn't present — is one of the most common and most overlooked forms of time theft. Because it relies on cooperation between workers rather than obvious deception, it often goes unnoticed for months or years.

The financial impact scales quickly:

- A company with $1,000,000 in annual payroll could lose $20,000 to $50,000 each year.
- A company with $5,000,000 in payroll could lose $100,000 to $250,000 annually.

In industries with thin margins, those losses can erase the profit on entire contracts — in overtime you didn't need to pay, hours you can't bill back to clients and labor costs that quietly inflate every invoice.

One important note: the absence of reported incidents is not proof that buddy punching isn't happening. Time theft is rarely visible without verification technology in place.

CHAPTER 2

# WHY DISTRIBUTED WORKFORCES ARE ESPECIALLY VULNERABLE

Security and cleaning companies face a higher risk of time theft than businesses with centralized operations, for straightforward reasons. Your people work where your clients are: across multiple sites, often without on-site supervision, particularly during overnight or weekend shifts. Shift changes require many people to clock in quickly at the same location. Environments like basements, parking structures and remote facilities add connectivity challenges that complicate traditional tracking.

For years, the standard answer to this problem was dedicated hardware like fingerprint scanners or specialized terminals installed at each job site. However, installing, maintaining and securing equipment across dozens of client locations is expensive, logistically difficult and clients may not permit it on their premises. This is why so many operators have continued to rely on PINs or paper.

Modern biometric solutions have changed that. By running on the smartphones and tablets your teams already carry, identity verification now comes directly to the field without any new hardware.

CHAPTER 3

# WHAT BIOMETRIC TIMEKEEPING ACTUALLY IS

Biometric timekeeping uses a unique physical characteristic — in this case, a person's face — to confirm identity when employees clock in or out. The system verifies that the right worker is physically present at the moment of the punch.

WinTeam Biometrics uses facial verification built directly into the WinTeam Mobile Time Clock. When an employee clocks in or out, they're prompted to take a quick facial scan, which is compared against a stored reference image of that specific employee. This is called one-to-one face matching.

The experience is designed to feel familiar: employees open WinTeam Mobile as they normally would, take a photo when prompted, and the punch goes through once the match is confirmed. If a biometric match falls below a configurable threshold, it is automatically flagged as an exception for supervisor review and no time data is lost.

A common question is whether someone could hold up a photo to fool the system. While this would technically be possible to do, every punch generates a permanent photo record with a confidence score that is silently captured. Because workers receive no indication of whether their photo passed or failed, the audit trail itself creates a powerful check on behavior. Any drop in match quality is automatically flagged for manager review. That added layer is what makes facial verification a genuine deterrent rather than a convenience feature.

One clarification worth making: WinTeam Biometrics is a specialized enterprise solution and does not use a device's native features like Apple's Face ID or Android's fingerprint scanner. It uses professional facial recognition technology from a third-party provider to deliver the accuracy that workforce management requires.

CHAPTER 4

# THE FEATURES THAT DEFINE A BEST-IN-CLASS SOLUTION

Not all advanced timekeeping tools are equal. As you evaluate options, look for the following capabilities:

- **Device flexibility.** The strongest solutions run on existing smartphones and tablets, removing the need for specialized hardware and simplifying onboarding.
- **Kiosk mode.** For high-volume shift changes, a single shared tablet can verify multiple employees quickly from a secure database.
- **GPS verification.** In single-worker mode, GPS confirms employees are at their assigned sites when submitting punches. In kiosk mode, a device can be anchored to fixed coordinates for consistent compliance tracking.
- **Offline capability.** Because teams frequently work in areas with poor connectivity, reliable performance without a network connection is essential.
- **Multilingual support.** The interface should be accessible for a diverse frontline workforce.
- **Configurable security thresholds.** Biometrics can be enabled for specific jobs, sites or devices — from "photo capture only" for high-volume areas in sensitive jurisdictions to "biometrically verified" for maximum-security sites.
- **Integration with payroll and scheduling.** A biometric tool that doesn't connect to your core platform simply trades one reconciliation problem for another.

CHAPTER 5

# PRIVACY, CONSENT AND COMPLIANCE DONE RIGHT

Collecting biometric data carries real responsibility, and a well-designed solution treats privacy as a foundation rather than an afterthought.

Before any worker uses the system, they complete a consent step, presented with a required notice before their first scan, with the option to accept or decline enrollment before any data is processed. Supervisors also have the authority to unenroll workers and permanently remove their biometric data when necessary, such as when an employee leaves the company.

Beyond protecting employees, this compliance framework creates a competitive advantage. Many security and cleaning contracts include requirements around verified attendance and accurate labor reporting. Documented consent workflows and a clear audit trail help you meet those requirements — and give you something concrete to point to when bidding on new work.

CHAPTER 6

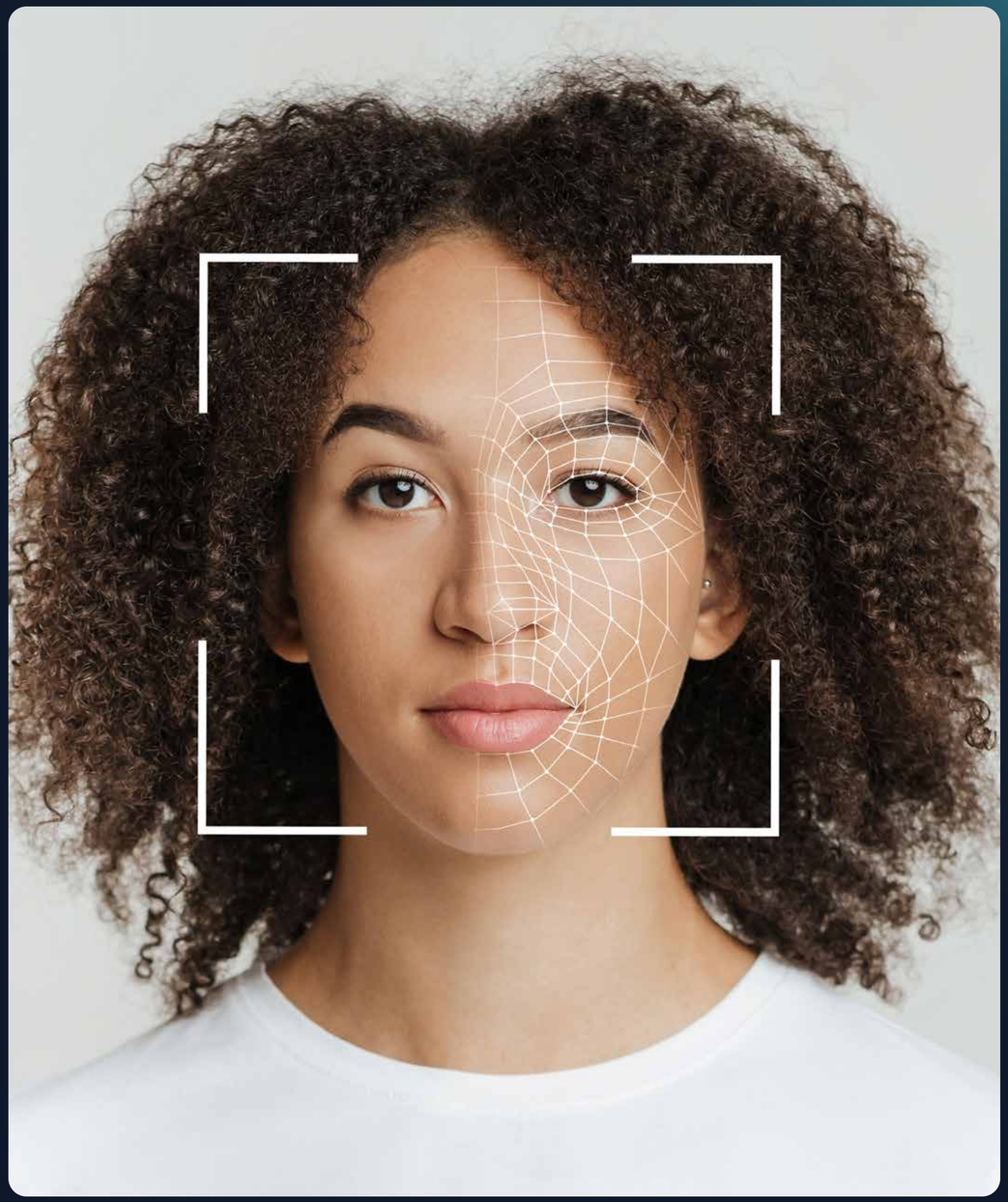
# IMPLEMENTATION — WHAT TO EXPECT

Biometric verification within WinTeam Mobile is built to fit into the punch flow your teams already use, which keeps the transition manageable. The process follows three phases.

- **Configuration.** Administrators set up kiosk devices and configure punch photo and biometric settings to match the security requirements of each site.
- **Enrollment.** Each employee captures an initial high-quality facial scan — the reference image used for all future identity matches. Employees can self-enroll or receive supervisor assistance at a kiosk.
- **Photo Capture.** Employees are prompted for a photo when clocking in or out. For employees enrolled in biometrics, an identity match confidence score is stored with every punch.

Once live, the day-to-day experience is straightforward. Employees are prompted to take a facial scan as part of their normal clock-in flow.

A phased rollout is generally the most practical approach. Starting with your highest-risk or least-supervised sites allows you to validate results before scaling company-wide.



CHAPTER 7

# MEASURING THE RETURN ON YOUR INVESTMENT

The most direct return from biometric timekeeping is payroll leakage recovery. Eliminating the 2–5% that time theft can drain from annual payroll often covers the cost of the solution on its own. But the full return extends further.

Supervisors spend significant hours each month reconciling time discrepancies, chasing missing punches and resolving disputes. Verified data at the source reduces that administrative burden directly. Fewer manual corrections also mean fewer payroll errors and a smoother processing cycle.

On the client side, a detailed audit trail for every shift gives clients confidence that billed hours were genuinely worked. That trust supports contract retention and strengthens your position when pursuing new business.


To build the internal case, three calculations are useful:

- Your annual payroll multiplied by 2–5% to estimate recoverable losses
- An estimate of supervisor hours spent monthly on time reconciliation and their associated labor cost
- An assessment of contracts where verified attendance is a stated requirement or competitive differentiator

**The total tends to make the decision straightforward.**

The greatest value comes when biometric verification is part of an integrated platform. When time and attendance data flows automatically into scheduling, billing and payroll, the manual reconciliation that creates errors and delays across the operation is eliminated at the source.

CONCLUSION

# VALIDATE YOUR TIME, PROTECT YOUR MARGINS

Buddy punching costs security and cleaning companies an estimated 2–5% of annual payroll, and distributed workforces are especially exposed because traditional verification has never been practical at scale. Biometric timekeeping with facial verification — and additional timekeeping tools including punch photos, GPS, kiosk mode, offline capability and multilingual support — now runs on the devices your teams already carry, with no expensive hardware and no disruptive new workflow to learn.

When integrated into a platform like WinTeam Mobile, verified time data flows directly into scheduling, billing and payroll, closing the gaps that drain both time and money from your operation.

Biometric verification is available in WinTeam Mobile — purpose-built for security and cleaning companies. To learn how it can fit into your operation, schedule a personalized demo with us today.

**Don’t just track your time. Validate it.**