VerifiedKnock: Officer Safety & Privacy Brief

Prepared for Police Union Representatives

The Core Promise: Safety Without Surveillance

VerifiedKnock is the first identity verification system designed with **Officer Privacy** as a foundational requirement. We understand that while officers need a way to prove their authority to the public, they should not be subjected to constant location tracking or invasive monitoring.

This document outlines how VerifiedKnock protects your members while enhancing their safety on duty.

1. No GPS Tracking (The "Outbound-Only" Model)

Most modern police tech (body cams, dispatch apps, radio systems) constantly pings the officer's location to a central server. VerifiedKnock is different.

- **How It Works:** Verification is a **peer-to-peer** handshake between the officer's device and the resident's phone via secure NFC/UWB.
- **The Privacy Guarantee:** The verification happens locally. The officer's device does **NOT** report GPS coordinates to a central database during this process.
- **Why It Matters:** Officers can prove who they are without creating a permanent digital breadcrumb trail of their every movement.

2. Automatic “Off-Duty” Protection

One of the biggest concerns for officers is the blurring of lines between “On Duty” and “Off Duty.” VerifiedKnock enforces a strict digital boundary.

- **The “Cinderella” Protocol:** Digital credentials are automatically set to expire at the end of the officer’s shift.
- **Zero Risk:** An officer cannot accidentally (or be pressured to) use their digital authority when off the clock. The system simply won’t work.
- **Liability Shield:** This protects the officer from accusations of acting under color of law during private time.

3. Hardware-Based Identity (No Personal Phone Usage)

We do not require officers to install invasive apps on their personal devices.

- **Agency-Issued Hardware:** The system works with agency-issued smartphones or dedicated **AuthenTrend Biometric Cards**.
- **Data Separation:** If an officer chooses to use a personal device, the app runs in a “Sandbox” mode that cannot access personal data (photos, contacts, browsing history).
- **Biometric Lock:** If a device is lost or stolen, it is useless to a criminal because it requires the officer’s specific fingerprint to unlock.

4. Reducing Confrontation Risks

Impersonation is a major threat to officer safety. When citizens are unsure if a “cop” is real, they are more likely to be defensive, non-compliant, or armed.

- **De-Escalation Tool:** By providing an instant, unforgeable proof of identity *before* the door opens, VerifiedKnock lowers the temperature of the interaction.
- **Silent Duress Signal:** In a worst-case scenario (e.g., an ambush), an officer can trigger a “Silent Duress” signal through the verification flow, alerting backup without tipping off the suspect.

Conclusion

VerifiedKnock is not a surveillance tool; it is a **safety shield**. It gives officers the power to prove their legitimacy instantly, without sacrificing their privacy or autonomy.

We invite Union Leadership to review our technical architecture and confirm these privacy protections independently.

Contact: [Your Name/Title] VerifiedKnock founders@verifiedknock.com