Extended Access Technology:

More Secure and Convenient Ways to Prove You're You

EBOOK

Contents

Introduction

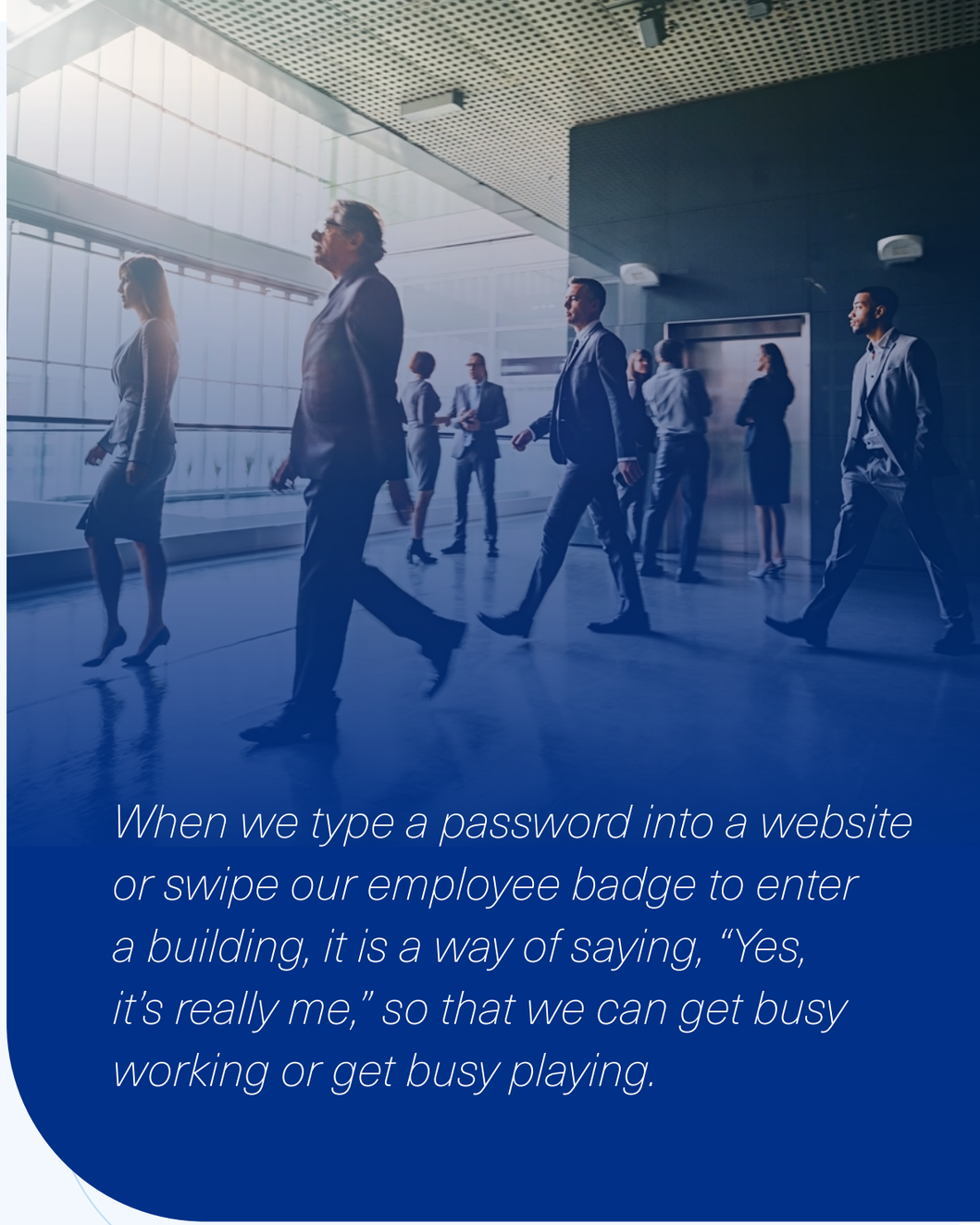
WHY FRICTIONLESS USER AUTHENTICATION MATTERS

Whether we are aware of it or not, we all spend a significant amount of time and energy each day verifying our identity and rights to access places and experiences in the physical and digital world.

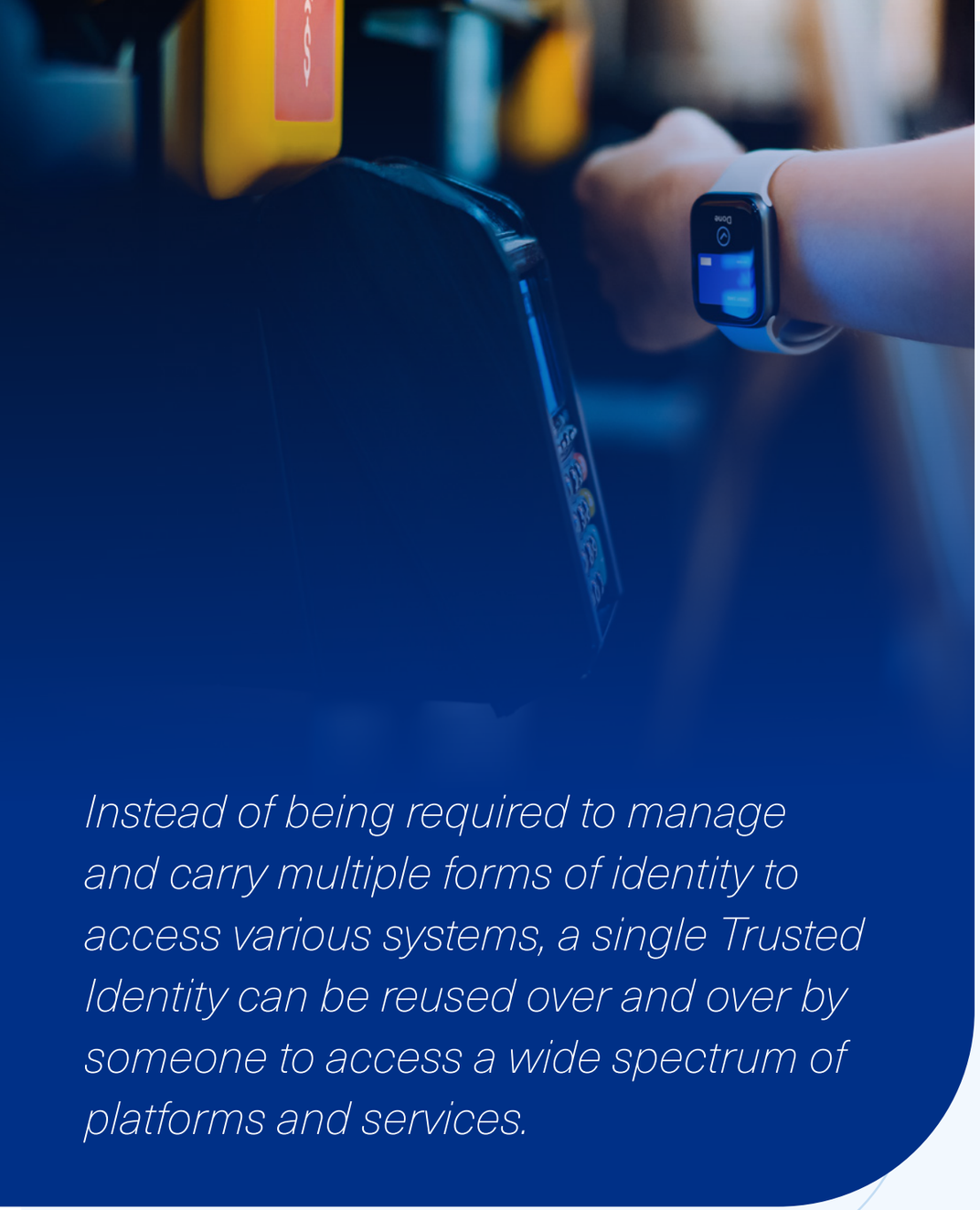
When we put a key into a car's ignition, that key indicates that we either own or have been granted access to that car. When we use a credit card or mobile phone to pay for a cup of coffee, that payment method is verifying that money will be removed from our bank account.

Ideally, we are able to move on from verifying our identity and right to accessing that service or location without a second thought. When there is a snag—a forgotten password, a misplaced key, poorly functioning technology—our day is interrupted. At an individual level, this can be a minor annoyance. At an enterprise level, this can mean a major financial expense, frustrated customers and unproductive employees.

Every day, millions of people in more than 100 countries use our products and services to securely access physical and digital places. Some of the world's most secure organizations rely upon our technology to protect their most sensitive resources. This short eBook is a compilation of some of the more innovative and surprising ways that HID Global Extended Access Technologies is harnessing the power of RFID to simplify and secure lives.



When we type a password into a website or swipe our employee badge to enter a building, it is a way of saying, "Yes, it's really me," so that we can get busy working or get busy playing.



Instead of being required to manage and carry multiple forms of identity to access various systems, a single Trusted Identity can be reused over and over by someone to access a wide spectrum of platforms and services.

Trusted Identities

ESTABLISHING A TRUSTED IDENTITY FOR SECURE AND CONVENIENT AUTHENTICATION WHERE AND WHEN IT MATTERS

The route to simple, secure user authentication begins with establishing a “Trusted Identity.” This Trusted Identity can exist as multiple form factors — like a card, smart phone, fingerprint or wearable device — in the same way that a reader (used to verify that identity) can be a desktop device or even embedded into or associated with nearly limitless systems and interfaces.

As more and more companies are offer flexible work schedules, consolidate and modernize their office spaces, and to meet demands for better user experiences, implementing seamless and stress-free user authentication is critical.

Although increased mobility can be associated with the exposure of additional vulnerabilities, it doesn’t have to. Using the right technology, there is no trade off between convenience and security.

Read on to learn more about the multitude of use cases that can be unlocked through a swipe, tap or mere presence of a Trusted Identity.

Want to dive deeper into the power of connecting multiple business systems?
Check out our executive brief, Experiencing the Connected Workplace: Seamless, Secure and Predictive.

Use Cases

USE CASE 1: ACCESS CONTROL FOR ELEVATORS, TURNSTILES & LOCKS

Controlling access to physical places is a critical security requirement. Employees, visitors, vendors and contractors move in and out through buildings all day long — each with distinct needs and necessary privileges.

Access control brings to mind fortifying building exterior perimeters, but there is so much more to it. Readers can be installed to control access and improve the flow within a building, including to these critical areas:

- Elevators
- Turnstiles
- Lockers
- Locked cabinets or secure areas (like server rooms or anywhere storing dangerous, sensitive or expensive materials)

When it comes to building lobbies, for example, security is paramount, but so is the rate at which people are able to enter and exit. Turnstile manufacturers are increasingly looking for solutions that include mobile access (the provisioning of a virtual ID credential onto a mobile phone) so that they are able to maximize security while keeping people moving throughout the hustle and bustle of a busy work day.

Curious about using mobile devices to gain access to secured doors, gates and networks?
Learn more here.

Ensuring that the right people have the right access at the right time, while keeping out the people who have no business being there, needs to happen seamlessly and with 100% certainty.

Fortunately, there are a number of ways to combat the practice of illegal clock-ins without adding any additional hoops to jump through.

USE CASE 2: TIME & ATTENDANCE

Buddy punching, the practice of clocking in for a coworker who is not actually working, is one of the most pervasive types of fraud and a costly issue for manufacturers and other organizations. According to Nucleus Research, up to 2% of a company's payroll is lost to buddy punching.

Linking a company's time and attendance system to its access control system is one best practice. If employees are already used to carrying around their company identification badges while at work, it's convenient to use this same ID to clock in and out.

Besides combating buddy punching, linking a secure authentication solution to time and attendance helps address payroll errors, other types of time theft, unauthorized time off, ineffective labor reporting and compliance with local work regulations. The ease of simply swiping a badge or mobile phone to record an employee entering or leaving school or work is a positive user experience and helps maintain productivity.

Other ways to make your time and attendance systems even more secure include adding:

- Mobile Access (the provisioning of an ID credential onto a mobile phone) — The same person who might be tempted to hand over their ID badge to a coworker to clock in might think twice about handing over their smart phone
- Biometric Authentication — Using your finger, face, or unique behavior to confirm identity
- Multi-factor Authentication (MFA) — A combination of something you have (card/token/device), something you know (pin/password), and something you are (biometrics)

Use Cases

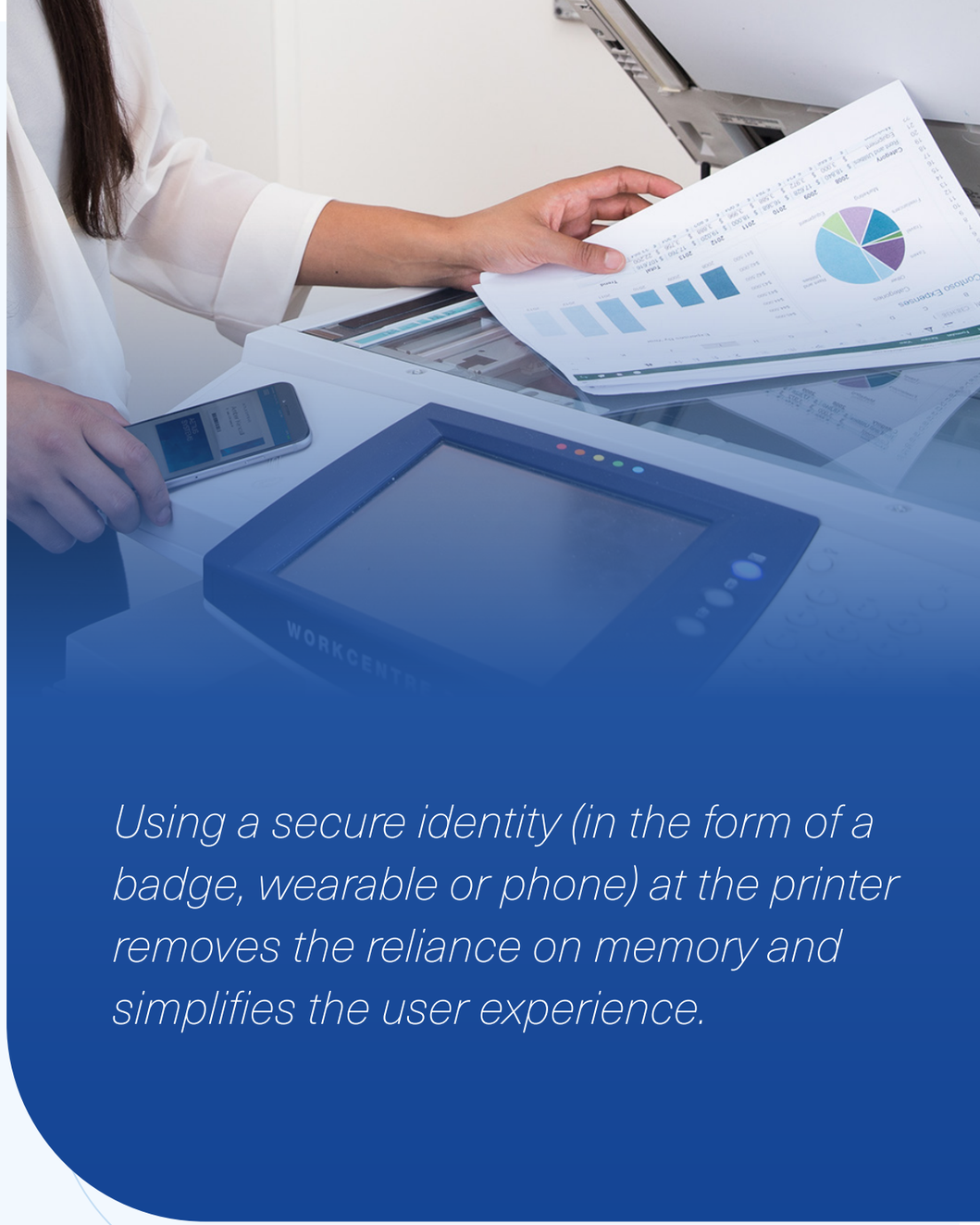
USE CASE 3: SECURE PRINT

Most of the focus on preventing major data and privacy breaches is placed on IT and digital systems, and the role of paper records can be easily overlooked. In addition to security concerns, untracked and unsecured printing is simply wasteful; many print jobs are never retrieved by the original user, racking up unnecessary paper and ink costs. With secure print, your organization can reduce unnecessary expenses and more accurately.

Even with the best of intentions, people can get distracted and forget to pick up a print job or mistakenly print a large document and not cancel it in time. Secure printing works by holding a print job at the ready until an authorized individual verifies their identity at the printer of their choice. No more hitting print on a confidential document and then racing to the printer to grab it. Some systems require a passcode before a sensitive document can be printed, but often these passcodes are lost or shared.

In addition to security concerns, untracked and unsecured printing is simply wasteful; 20% of print jobs are never retrieved by the original user,[3] racking up unnecessary paper and ink costs. With secure print, your organization can reduce unnecessary expenses and more accurately allocate costs—while saving the planet.

For technical details on implementing secure print at your organization, read our white paper, Implementing Secure Print.



Using a secure identity (in the form of a badge, wearable or phone) at the printer removes the reliance on memory and simplifies the user experience.

1. BakerHostetler 2017 Data Security Incident Response Report https://f.datasrvr.com/fr1/617/83514/2017_Data_Security_Incident_Response_Report_-_FINALpdf.pdf

2. Nuance research: https://whatsnext.nuance.com/office-productivity/orphaned-print-jobs-silent-security-leak/

While biometric technology can serve a variety of use cases, there are unique challenges to implementing it in healthcare environments.

USE CASE 4: PATIENT IDENTIFICATION & IMPROVED CARE

Many medical facilities still rely on simple bar code ID bracelets to identify patients, which are inexpensive but can be easily swapped or duplicated. With an increased need to combat identity theft fueled by rising costs and insurance fraud, hospital administrators are seeking more comprehensive and secure solutions.

For one, hospitals serve diverse populations—patients come in all different ages and ethnicities and sensors need to effectively obtain data quickly for everyone. Hospitals are also kept cool and dry, an environment that contributes to dry skin, creating difficultly for certain types of fingerprint readers. Finally, healthcare involves time-sensitive and patient-critical situations, requiring any biometric solution to detect a user quickly and consistently.

Besides patient identification, there are many opportunities to improve patient care and security by utilizing Trusted Identities, including:

- Ensuring that the right dosage of medicine is being dispensed to the right patient
- Limiting and tracking the access to commonly stolen medicines (like opioids and amphetamines) via smart locks on cabinets or storage areas
- Compliance with Electronic Prescription of Controlled Substances (EPCS) requirements
- Simplifying logical and physical access control, with a single credential that grants healthcare providers access to sensitive areas and patient records

Use Cases

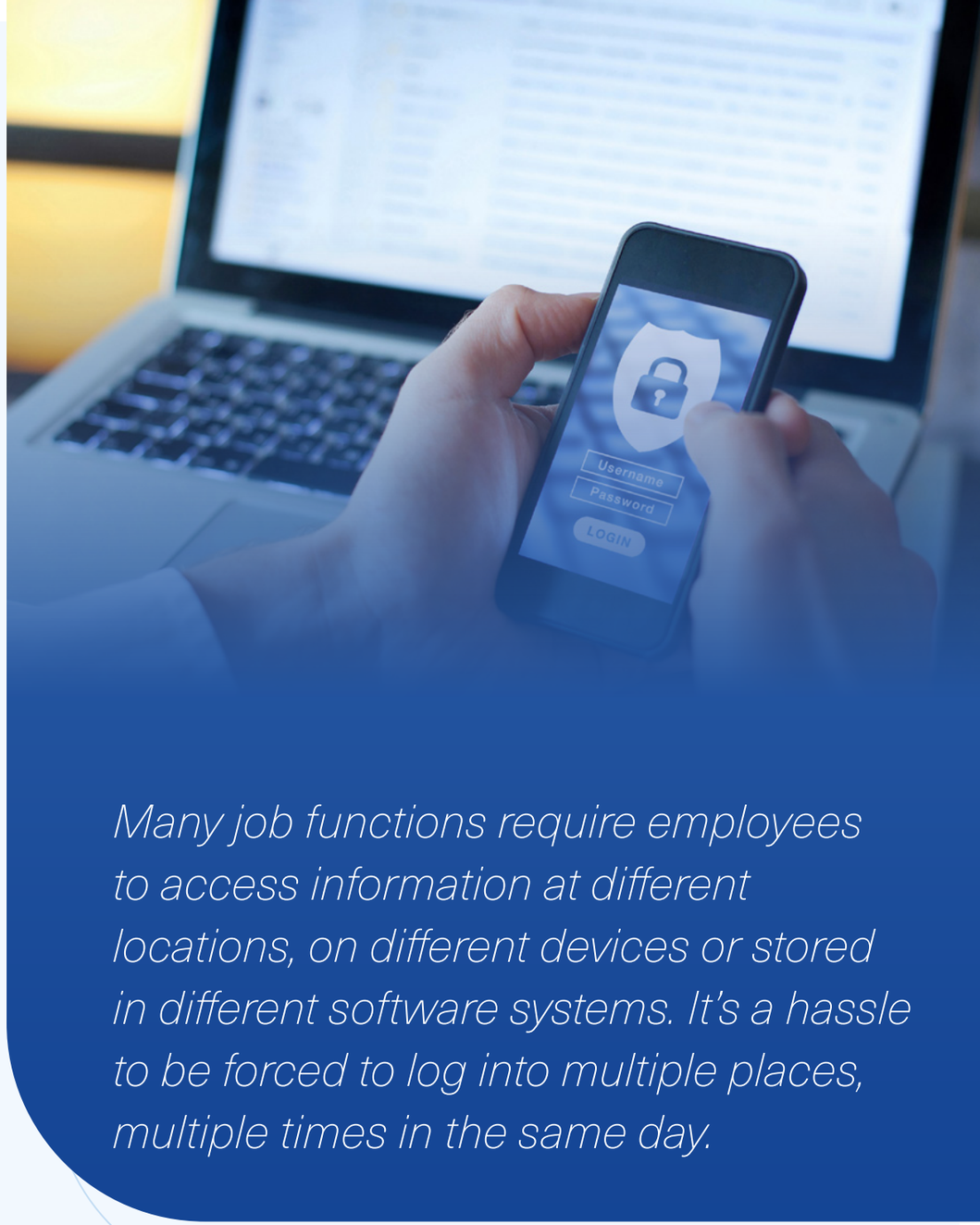
USE CASE 5: SINGLE SIGN ON (SSO) FOR DESKTOPS AND DEVICES

The way we work is changing. It's becoming less common to have one employee assigned to one desk or office, all the time.

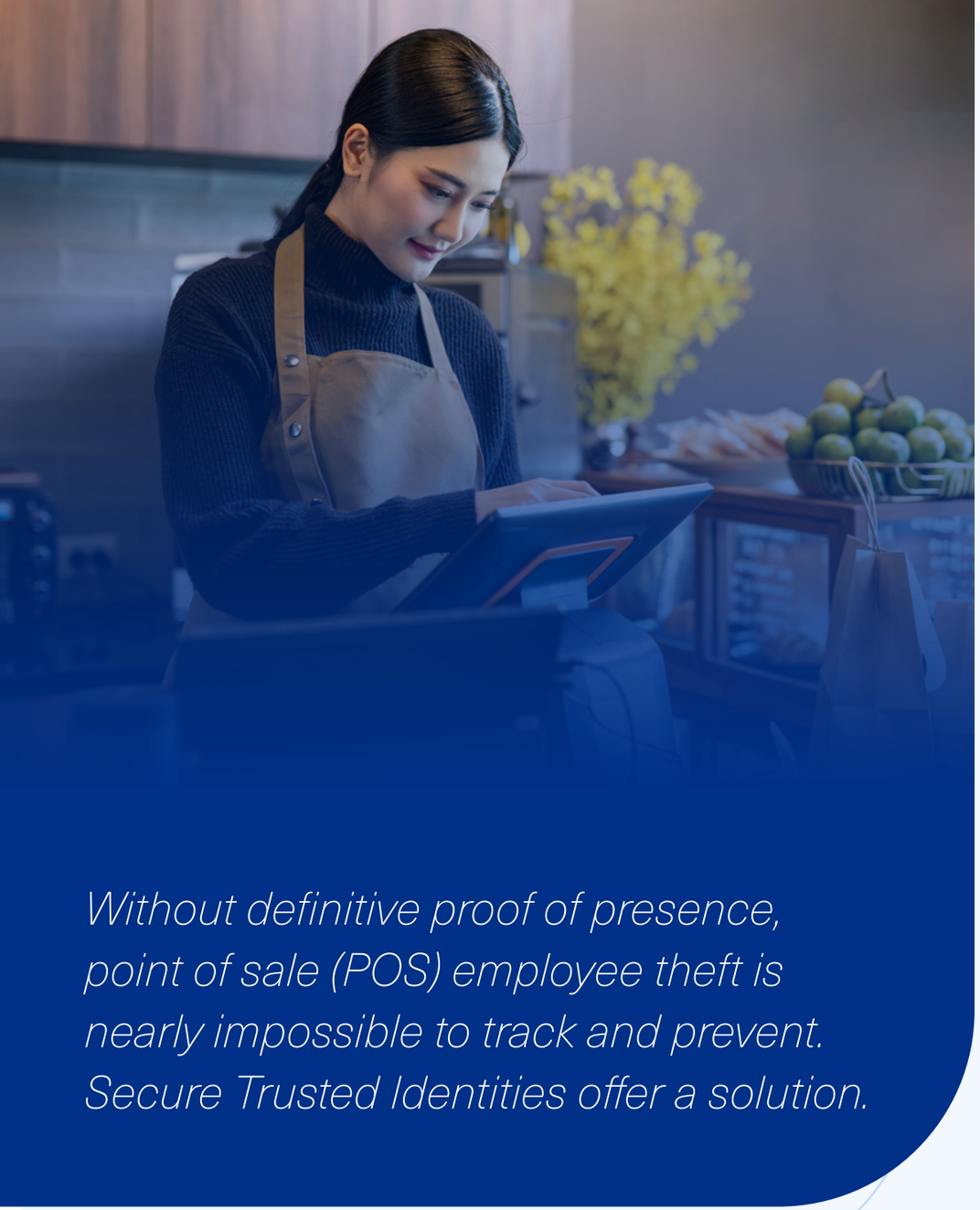
Single sign-on (SSO) allows people to use one master password to authenticate their identity at the beginning of a work period, granting secure access to the right software, files and locations without missing a beat. SSO also reduces IT support costs because there are fewer calls to the service desk for password resets.

One criticism of SSO is that if a password is compromised by a hacker or malware, it exposes multiple systems to that vulnerability. However, this risk is easily mitigated by combining SSO with multi-factor authentication (MFA). MFA is the use of several different factors — something you know, something you are and/or something you have, like a hard token — to verify a person's Trusted Identity before granting access.

To get a better understanding of how SSO and MFA can work together,
check out this blog post.



Many job functions require employees to access information at different locations, on different devices or stored in different software systems. It's a hassle to be forced to log into multiple places, multiple times in the same day.



Without definitive proof of presence, point of sale (POS) employee theft is nearly impossible to track and prevent. Secure Trusted Identities offer a solution.

USE CASE 6: RETAIL POINT OF SALE (POS)

Employee theft remains a serious problem for retailers — often costing more than theft from traditional shoplifters or outside organized retail criminals.

Because of this, it is difficult to determine who is accessing the POS system and responsible for specific transactions. However, by integrating an RFID or biometric reader with existing POS systems, retailers can be assured who is responsible for any given transaction. In addition, by using the same readers to log in employees to their assigned shifts, they can also monitor time and attendance with superior levels of accuracy and confidence.

Here are a few of the risk factors that can be eliminated using an RFID or biometric solution at the retail point of sale, such as HID DigitalPersona® or HID OMNIKEY® desktop readers or modules:

- **Inventory Shrink —** Unauthorized voids, refunds, returns, discounts and fraudulent gift card transactions
- **Time & Attendance Fraud —** Tardy arrivals, buddy punching, lollygagging, extended breaks and early departures
- **Unnecessary IT Costs —** Provisioning and replacing cards/tokens, and issuing password resets

Solutions

EXTENDING THE REACH OF HID GLOBAL'S TRUSTED IDENTITY TECHNOLOGY

To create a comprehensive view of every way in which our Extended Access Technologies can be put to use is an impossible task. From border control to airline check-ins, voter and government benefit programs to cafeteria and vending machine payments — the list is growing all the time.

- **OMNIKEY Smartcard Readers**
- **OMNIKEY Reader Modules**
- **iCLASS SE Modules**

Or visit hidglobal.com/extended-access-technologies.

Ensuring that the right people have the right access at the right time, while keeping out the people who have no business being there, needs to happen seamlessly and with 100% certainty.

hidglobal.com

North America: +1 512 776 9000
Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800
Latin America: +52 (55) 9171-1108

For more global phone numbers click here

2022-02-04-eat-more-secure-convenient-ways-en-eb
PLT-06385

Part of ASSA ABLOY