

## IdentityCare: The Most Secure Digital Identifier for SaaS

*An IdentityCare White Paper*

*"The next generation of digital identity technology is a necessity for the growth, privacy and security demands of this new era."*

*– 1414 Ventures*

The need for a next-generation digital identity (digital ID) is growing. More and more, the limitations of passwords and single digital identity sign-on are resulting in compromised data. Consumers want an easier yet more secure way to log into websites and apps for everything from banking, insurance, healthcare, and e-commerce to business applications and data access. IdentityCare solves these challenges with something people always have with them...their face, and more specifically, their epidermis.

### The Problem

There is arguably no greater business problem today than the threat of identity fraud and cyber-attack. There has been no effective solution that leverages a person's unique physical traits without the need for photographs or scans that can be hacked and used to steal a person's identity. The legacy biometrics used in a one-to-one (1:1) identity verification mode today are all based on "things we leave behind", such as photographs and fingerprints. An alarming increase in cyberthreats and financial fraud has led government and industry to call for new solutions.

In 1995, the year EBay and Amazon gave most people their first good reason to put personal information online, there were around 9,000 cases of identity fraud reported in the US. In 1998<sup>1</sup> the Government Accounting Office (GAO) reported to Congress that while identity fraud existed to a minor degree, most of it was related to crimes ranging from illegal driver's licenses to credit card theft and it was typically not tracked by law enforcement.<sup>2</sup>

By 2002 the GAO's message had changed. This growing universe of identity theft was largely unknown. There were no readily available statistics on the prevalence of identity theft. Victims may not know they are victims and may choose not to report the incident if they did know. Estimates ranged from one-quarter to three-quarters of a million victims annually, with no factual basis to gauge assumptions. Federal law enforcement agencies had no way to facilitate tracking of identity theft cases. The FBI and Secret Service noted that identity theft was often a component of white-collar or financial crimes.<sup>3</sup>

Fast-forward two decades. In 2023 there were more than 350 million victims of identity fraud in the US (population 340 million) with 97% of them attributed to cyber-attacks.<sup>4</sup> This represents a 78 percent increase over the previous year and a 72 percent hike from the previous all-time high number

---

<sup>1</sup> Congress would enact the Identity Theft and Assumption Deterrence Act of 1998 aka the Identity Theft Act later in 1998 Public Law 105-318. The relevant section of this legislation is codified at 18 U.S.C. § 1028(a)(7)

<sup>2</sup> GAO Briefing Report to Congressional Requesters May 1998 "Identity Fraud: Information on Prevalence, Cost, and Internet Impact is Limited."

<sup>3</sup> GAO Briefing Report to Congressional Requesters March 2002 "Identity Theft: Prevalence and Cost Appear to be Growing."

<sup>4</sup> See Identity Theft Resource Center 2023 Data Breach Report page 5 "Total Compromises in 2023."

of compromises (1,860) set in 2021. In 2023, Wells Fargo spent \$1.7B on Risk Mitigation Infrastructure.

Many solution vendors are focusing on balancing UX convenience with secure transactions. Ongoing customer demands for self-sovereign identity (i.e., sole ownership and control over personal data) continues to drive biometric authentication's evolution. The post-COVID-19 world requires a higher level of remote, contactless transactions, driving the need for accurate and efficient identity authentication. Currently, biometrics are considered suitable for verification of identity as a secondary credential only, due to concerns with accuracy, bias, spoofing, and a general lack of secrecy resulting in theft. As a result, conventional facial recognition technology companies such as Idemia or Alcatraz.ai focus on surveillance, AI, and 1:1 and/or secondary verification.

## The Solution

IdentityCare provides a next generation modular digital identifier for SaaS. This unique, proprietary biometric performs as a one-to-many (1:N) authenticator of identity, the attestation and non-repudiation components of user authentication associated with a wide array of transactions at a fraction of the current cost of fraud. The modular credential is containerized in a docker stack for application in a SaaS environment. IdentityCare is positioned to be first to market as a patented FIDO2-compatible 1:N biometric credentialing solution for zero trust. This allows for predictable, recurring revenue rather than one-time sales and periodic software upgrades. Just as customers may use DocuSign® or malware protection software, clients will be able to use IdentityCare software with containerized biometric authentication as one identity management credential to replace passwords, pins, and other unreliable forms of identification. IdentityCare's 1:N capability promises substantial convenience value proposition for both customers and employees, increasing the likelihood a sustaining initial and profit margins above 40%. In the one case of Wells Fargo (per above), deploying IdentityCare across its 238,698 employees would cost less than \$24M a year, or .014% of the \$1.7B.

IdentityCare's unique epidermis biometric embodies the essential qualities of all three NIST authentication methods: Type 1 "something you know", Type 2 "something you have", and Type 3, "something you are".<sup>5</sup> The technology includes an identity credential based on data that is secretive in nature that can be readily collected from anyone who opts-in and only used to identify that person within the IdentityCare modular system.<sup>6</sup> Outside the system IdentityCare biometric data is meaningless, thus creating a safe and secure digital identity credential.

## How It Works

IdentityCare's next generation biometric is enterprise vetted, contains no PII, is spoof resistant (a "secret biometric" taken from the epidermis), protects user privacy, and meets growing legislative measures on data privacy and AI. To look at how IdentityCare works, we will examine:

- a) the Biometric Signature Data,
- b) how IdentityCare protects the user, sd
- c) the user experience,
- d) the importance of a one-to-many (1:N) credential,
- e) biometric solutions used in enterprise,

---

<sup>5</sup> See NIST Special Publication NIST SP 800-63B-4, Digital Identity Guidelines Authentication and Lifecycle Management 5.1.1. "Memorized Secrets."

<sup>6</sup> IdentityCare provides a digital identity that cannot "be obtained online or, in the case of a facial image, by taking a picture with or without their knowledge..." Id., 5.2.3 "Use of Biometrics," I. 1268.

f) and the impact of passkeys.

a) Biometric Signature Data

IdentityCare's Biometric Signature Data, or BSD, is the biometric data file used to identify the user. Millions of epidermal data points are collected from a participating user's face in an instant using a near-infrared light source. Proprietary algorithms discard all but around 5% of this data in the creation of an extremely accurate biometric identifier which, as a result, contains no personal information (PII). It does not resemble the user in any way and does not contain any PII but can still be used to accurately authenticate an individual.

Enrollment takes less than 15 seconds. Subsequent authentication takes less than a second. Only a live read of a user (who has opted into the system) using IdentityCare proprietary algorithms can match the BSD template of the user.<sup>7</sup> This proprietary, patented near-infrared authentication technology has been tested and deployed by 45% of the Fortune 100. It has never been hacked, spoofed, or allowed a false entry, providing reliable and accurate frictionless biometric access. IdentityCare technology is based on well-understood principles of physics and does not rely on an AI "black box" to enhance accuracy, neither can AI be used to spoof IdentityCare BSD. IdentityCare is also a FIDO2-compatible biometric solution ideally suited for passkey requirements. As a 1:N biometric primary credential, multiple users can be authorized to operate or interact with varying privileges with devices, appliances, furniture, vehicles, buildings, and online.

The strength of a digital ID based upon the user's distinct characteristics is fundamental to creating the needed credential. The authorized user's face is analyzed for the distinctiveness of comparative features to create that person's unique access key ("IdentityCare credential"). Layered reinforcement is applied which overlays several layers of different size "pixel boxes" on the facial image in a way that has an amplifying impact on the analysis of the face. Areas that are exceptionally unique to the face are emphasized, and areas that are more common between faces are deemphasized. This 'layered reinforcement' of the unique characteristics of the face is proprietary to IdentityCare technology and results in significantly increased accuracy.

IdentityCare data is fully encrypted and managed within a complete, integrated biometric-centric environment that creates a full audit trail to mitigate risk and assures with the asynchronous encryption based upon the biometric access key that only the user be permitted to access the protected data. Such biometric credential-based encryption allows for cost savings, risk mitigation, and a decrease in the need to harden the entire environment from cyber intrusion. Opportunities include the deployment of encryption based upon the user's BSD, attestation and removal of hardened data centers and infrastructure.

b) Protecting the User

When it comes to how a Zero-Trust credential protects against fraud, ask:

1. can it be used to identify me? (does it contain recognizable PII?)
2. can it be used to spoof me? (can it be used to imitate me and commit fraud?)

Either one is bad; together they spell disaster. By harnessing advanced secure biometric solutions utilized for years in enterprise physical access control by its partner StoneLock, the IdentityCare platform protects and facilitates user's Personally Identifiable Information (PII) in

---

<sup>7</sup> ITRC Biometric Working Paper, "Data alone Can No Longer Be Trusted as the Sole Source of Truth About a Person's Identity," November, 2023.

compliance with emerging global legislation such as Biometric Information Privacy Act(s) (“BIPA”) requirements adopted by several states and the 2018 GDPR and AI standards being enforced in the EU with increased penalties.<sup>8</sup> IdentityCare’s dynamic templates also do not use images, pictures, geometry, facial distance, or other standard FR techniques argued to produce gender and race bias and increase likelihood of spoofing.

IdentityCare is the also the first biometric to provide attestation and non-repudiation of user authentication associated with a transaction. And in an age only beginning to test the limits and consequences of AI, IdentityCare does not employ an AI “black box” that cannot be explained. This is because the ability to audit is both an integral component and function of attestation. Other biometrics implement AI to improve accuracy by learning data, which also may be a potential violation of privacy law depending on the data used.

#### c) The User Experience (UX)

The facial recognition industry has matured over the past decade, with the introduction of 1:1 FaceID on the iPhone gaining facial recognition widespread acceptance. As technology matures, it demands a better user experience (UX) – for example the experience of conveniently unlocking an iPhone - in order to gain acceptance. When it comes to the UX, Steve Jobs famously said “You’ve got to start with the customer experience and work backwards to the technology, not the other way around.”

IdentityCare technology was designed and vetted through generations specifically to create a nearly-transparent UX – as important as speed and accuracy. Self-enrollment is a simple 15-second process initiated by presenting a QR code. The UX is designed to intuitively guide a user into optimal alignment, overcoming accuracy issues faced by biometrics associated with a poor read, such as iris scans that suffer from variances in lighting conditions, or finger “waves” that scan multiple fingers to mitigate read errors.

IdentityCare biometric devices operate in an entirely touch-less environment (unlike fingerprint readers and other biometric devices) that is even more important in this post-COVID 19 world. IdentityCare is designed to be an instantaneous, virtually frictionless user experience. A frictionless user experience is heavily dependent on speed and accuracy resulting in a superior solution performance: matching accuracy greater than 98% with less than one second of user interaction with the system.

A traditional problem with biometrics has been the enrollment process and credential management. Utilizing a QR code or card swipe, the easy-to-read display guides users through a simple and touchless self-enrollment process. Opt-in enrollment is easy, requiring only 15 seconds to register a new user at any device on the network by simply presenting a QR code to the reader. Subsequent authentications of that user require less than a second and no contact with the edge device.

#### d) 1:1 vs 1:N Identification

A 1:1 comparison is a verification of identity. Over the past decade, 1:1 biometrics have proven an effective alternative to the problems associated with passcodes on mobile platforms and computers, improving the user experience by allowing for quick, convenient access. In most mobile devices sold today, a 1:1 comparison is used to detect the phone’s owner, providing a binary ‘yes or

---

<sup>8</sup> By year-end 2024, Gartner predicts that 75% of the world’s population will have its personal data covered under modern privacy regulations. Nader Henein, VP Analyst at Gartner.

no' response to the question "is it my owner or not?" Mobile devices are designed to authenticate one owner, the primary user. Current biometrics in the role of 1:1 verification of identity are prone to some error but provide acceptable levels of intrusion deterrence and convenience for individual devices.

A 1:N comparison is an authentication of an identity. A 1:N biometric, meaning "one to many" makes a comparison of one user against an entire database of users, thousands or millions of records attempting to authenticate the user. A 1:N biometric primary credential used as a passkey (see passkeys below) would allow thousands or millions of authorizations to operate or interact with varying privileges with devices, appliances, furniture, vehicles, buildings, and online.

#### e) Biometrics in Enterprise

Enterprise systems present more complex issues, as by their definition they comprise various people, types of information and varying technology working in concert. As such, 1:1 biometrics are used to a much smaller degree in enterprise access control for secondary authentication coupled with the primary authentication card or pin number.<sup>9</sup> The solution for enterprise is a 1:N, or 'one-to-many' comparison is able to answer "is it anyone I know" yes or no in the context of 1 against many. A 1:N comparison is therefore the fundamental characteristic of a primary biometric credential capable of replacing cards, passcodes, and pin numbers. As stated above, anything else is 1:1 verification. At the enterprise (and government) level, a 1:N biometric primary credential would allow for:

- the elimination of security access cards
- secure financial and other digital transactions
- secure document transmission/reception
- secure tax returns
- secure ballot casting
- passkeys requiring attestation for SaaS transaction models

### Passkeys

In March of 2022, FIDO ([fidoalliance.org](https://fidoalliance.org)) announced a cross-platform standard for eliminating passcodes once and for all computers and mobile devices in favor of a biometric asynchronous key or "Pluggable Authorized Biometric" under FIDO guidelines. This standard is applicable to all biometrics, and was immediately adopted by Apple, Google, and Microsoft. The FIDO standard tells us two things:

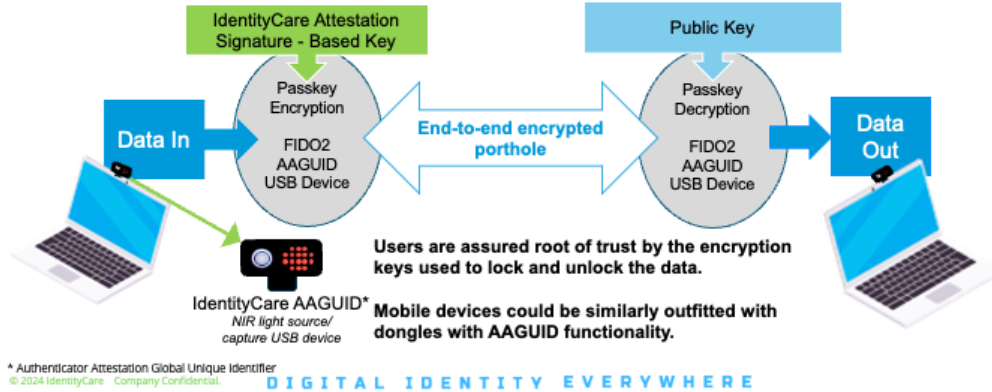
First, the future is now set to move away from passcodes to biometrics. Previously speculated, now we have the roadmap. The largest companies in the world agree and have all adopted FIDO2 passkeys to replace the passcode. Second, there is now an industry standard by which StoneLock's technology, previously limited to the Physical Access Control space, can suddenly be applied to the much larger Identity Management space as a containerized SaaS solution. For example, IdentityCare could be incorporated into the entire Google Chromebook hardware line, allowing users instant access to their Google suites from any device; the same could be achieved with Microsoft products, or inside a Meta VR headset for purposes of secure user authentication while in the Metaverse. Such authentication could instantly be harnessed by the likes of Facebook or X (formerly Twitter) or Uber or any of the digital platforms that plagued with authentication-based fraud. These massive implementations could be achieved by any of these companies relatively quickly by either licensing or acquiring IdentityCare's significant patent portfolio and trade secrets developed over the last decade.

---

<sup>9</sup> No biometric before the IdentityCare credential has ever demonstrated the accuracy or reliability to be used for anything other than secondary verification in enterprise access control.

## IdentityCare Solutions: Passkeys

- The FIDO2 Passkey is a digital attestation standard replacing passwords.
- Passkeys validate identities with digital attestation signatures verified by public keys.
- IdentityCare’s solution uses biometric attestation data as the encryption key, assuring *root of trust*.



## TECHNOLOGY AND INTELLECTUAL PROPERTY OVERVIEW

IdentityCare holds IP in the areas of use of NIR biometrics with asynchronous keys, elements of 1:N architecture (dynamic templates and collision detection), and privacy. To provide IP protection to assert against others and ensure licensing revenue, IdentityCare relies first upon U.S. patent(s) filed in 2012 based upon the creation of asynchronous credential keys from biometric information. Subsequent US utility patents were filed as continuations, or continuations in part to avoid publications/products prior to 2012 to create multiple points of protection should one patent be found to be invalid or not infringed, and ultimately to become part of larger systems/apps such as the “Pluggable Authorized Biometric” within FIDO2 standard adopted by Apple, Google, Microsoft.

### Patent Protection:

IdentityCare protects its technology with 15 US patents to-date) and similar foreign patents/applications that cover the use of an edge device (US 11,017,212 patent), non-visible light (US 11,017,211 patent), and algorithms (US 11,017,213 patent) that compare the distinctiveness of adjacent pixels using up to three ranked arrays (US 11,017,214 and 11,163,983 patents) to create a dynamic template (US 11,163,984 patent) containing biometric signature data (asynchronous credential key)(US 9,740,917 and 10,438,053 patents) that cannot be used to identify unknown persons (avoiding privacy concerns)(US 11,275,929 patent) but may be used for 1:N authentication (US 10,853,630 and 11,301,670 patents) for numerous users at multiple sites through a Gateway (US 11,017,211 patent), including outdoor environments (US 11,651,623)(expires 12/06), and use of non-visible light (US 11,594,072). IdentityCare may also rely on 2 issued U.S. design patents covering biometric edge capture devices (US D 932,489 and D 976,904 patents). Patent protection is deeply ingrained into the culture and everyday operations of IdentityCare and its partners.

### Intrinsic Privacy:

Pending federal and state legislation along with enhanced GDPR enforcement and recent EU AI Act will continue to impact facial recognition while highlighting how IdentityCare processes provide a competitive solution. See patent list below. Identity Care technology protects user privacy without demonstrating gender/race bias because the patented algorithms measure distinctiveness of adjacent

pixels at the subdural level collecting 2165 data points using non-visible light (rather than calculations based upon pictures or video) to produce a “heatmap” that cannot be used to identify ethnicity, gender, or other visible identifying features. This makes IdentityCare solutions both standard and stable across several application environments previously not possible with other biometric solutions.

Equally as important, this makes our biometric signature data incompatible with more conventional photographic or video-based facial recognition systems, thus helping to further ensure user privacy. These non-infrared facial recognition algorithms are designed to work with current security video monitoring systems, attempting to identify a face reliably from a photograph or video frame, perhaps at a distance or in a crowd, or even from someone who may not want to be identified. For both intrinsic and extrinsic reasons, those types of facial recognition are difficult to manage and do not achieve very high accuracy - typically testing in the 45-65% range. These variables all play a significant role in the performance accuracy and reliability of every non-infrared biometric system on the market today. In addition to being stored with the end user, the user templates deployed by IdentityCare are unusable to identify a person outside its system as recognized in the new intrinsic privacy '929 patent.

US 9,740,917 patent, issued 8/27/2017, Biometric Identification System and Methods  
US 10,438,053 patent, issued 10/08/2019, Biometric Identification etc.  
US 10,853,630 patent, issued 12/01/2020, Methods/Apparatus for Biometric Verification  
US 11,017,211 patent, issued 5/25/2021, Methods/Apparatus for Biometric Verification  
US 11,017,212 patent, issued 5/25/2021, Methods and Apparatus for Biometric Verification  
US 11,017,213 patent, issued 5/25/2021, Methods/Apparatus for Biometric Verification (Algos)  
US 11,017,214 patent, issued 5/25/2021, Methods/Apparatus for Biometric Verification (3-array algo)  
US 11,163,983 patent, issued 11/02/2021, Methods/Apparatus for Aligning Sampling Points of Facial Profiles...  
US 11,163,984 patent, issued 11/02/2021, Methods/Apparatus for Constructing Biometric Templates...  
US 11,275,929 patent, issued 3/15/2022, Methods/Apparatus for Privacy Protection During Biometric Verification  
US 11,301,670 patent, issued 4/12/2022, Methods/Apparatus for Collision Detection in Biometric Verification  
US D932,489 patent, issued 10/05/2021, Edge Device  
US D976,904 patent, issued 1/29/2023, Edge Device  
US 11,594,072 patent, issued 2/28/2023, Methods/Apparatus for Facial Recognition 3 Array Privacy Protection  
US 11,651,623 patent, issued 5/16/2023, Methods/Apparatus for Outdoor Access Control Using Biometrics  
AU 202113610, 6/16/2021 registered  
AU 202113611, 6/16/2021 registered  
CA 204269, 4/11/2023 registered  
EU 008581813-0001, 6/18/2021 registered  
EU 008581813-0002, 6/18/2021 granted  
GB 6143519, 6/18/21 registered  
GB 6143520, 6/18/2021 registered  
EU 020769474.6-1207, 2/08/2024 granted

## Sales and Marketing

By fulfilling a critical missing attestation component in SaaS and Zero-Trust, we believe IdentityCare is potentially disruptive to every sector of 1414's Digital Identity Opportunity Matrix.<sup>10</sup>

---

<sup>10</sup> <https://www.1414ventures.com>

IdentityCare will impact companies in that market everywhere by strengthening and verifying identity while complying with privacy legislation throughout the world. IdentityCare is a transformative solution in the digital identity verification market, offering a secure, reliable, and compliant biometric ID for Enterprise across platforms. It bridges the critical gap in the current digital identity space by leveraging near-infrared biometric technology, providing a more accurate, user-friendly, and fraud-resistant alternative to traditional identity verification methods. With a focus on hardened security through utilization of a zero-trust biometric credential, regulatory compliance, proven accuracy, intrinsic privacy, seamless integration, reliability, global scalability, and customer convenience, IdentityCare sets a new standard in digital identity verification. The unique value proposition, combined with strategic partnerships and a solid pipeline of prospective clients, positions IdentityCare for significant growth and market penetration in the rapidly evolving digital identity landscape.

Revenue is obtained via SaaS models, with subscriptions primarily sold to institutions, corporations, and governments, with end-user access provided at little to no cost. The revenue model is diversified, encompassing SaaS subscriptions, usage fees, licensing fees, channel sales, and opportunities presented by applications on the containerized edge. The idea is to remain scalable and flexible addressing the varying needs of large enterprises and government entities with a modular solution where one identity credential fits if not all, most. Recognizing that the identity credential is used within varying customer systems, the revenue model also includes professional services and support fees for providing customized integration for optimal security and performance.

1414 Ventures, an investment firm focused on Identity, measured the overall digital identity market at \$763 Billion in 2021 and projects \$1.01 trillion by 2025, encompassing various sectors such as retail, eCommerce, healthcare, government and defense, financial services, and more. Within this broad larger digital identity market, IdentityCare's credential is applicable to most of 1414's recognized 18 sectors. Targeting key sectors in the US, such as banking, healthcare, pharmaceutical and data enterprises, IdentityCare aims for a service addressable market with a conservative estimate of achieving a 10% market share. This is backed by a significant compound annual growth rate (CAGR) of 16%+, highlighting the rapid growth and demand in the facial recognition and digital identity sectors.

IdentityCare's go-to-market strategy leverages both direct sales to consumers through marketing and a B2B enterprise approach via partnerships, including value-added resellers (VARs), system integrators (SIs), and hardware vendors. The Company is engaging with experienced SaaS and cloud sales professionals. This multi-channel strategy ensures broad market penetration across targeted industries while ensuring product viability and predictable performance. The direct sales approach is complemented by strategic partnerships, enhancing the solution's reach and scalability across essential sectors.

IdentityCare recognizes that the Federal government has set and will continue to set standards for digital identity management that the private sector must comply with to compete for contracts as directed by several Executive Orders and NIST rulemaking discussed below. With that in mind, IdentityCare will focus on penetrating the public sector incorporating the US Federal Government's Zero Trust Mandate.

IdentityCare promotes privacy and the security of personal data:

- Create multiple levels of security with ID credentials.
- Provide 1:N for federal space.
- Audit trail establishing adherence to minimum cybersecurity requirements.
- Allows for the easy implementation of encryption (including the use of asymmetrical keys based upon identity asset) and authentication based upon the identity credential.
- Ensures critical systems are protected from unauthorized physical access and cyber threats.

IdentityCare is a modular key based upon a proprietary 1:N biometric that is adaptable throughout the varying cyber-sophistication of the Federal networks, similar to NameGrabber that allows Navy database to communicate with Marine Corps. It can help organizations transition to modern, secure networking architectures and systems while maintaining strict security and compliance requirements.

IdentityCare's dynamic templates also do not use images, pictures, geometry, facial distance or other standard FR techniques that have been argued to produce gender and race bias. Because IdentityCare's biometric authentication does not store data, various public and private users can adapt scale to their disparate platforms.

These software solutions are compliant with NIST standards forming the mandated template for federal contract as driven by Executive Order 14028 and emphasized in the White House National Cybersecurity Strategy, March 2023. Similar emphasis is growing in other sectors, including bolstering data protection in line with DHS IT Strategic Plan 2023, Goal 6, DHS Biometric and Identity Technology Center, DHS Office of Biometric Identity Management (OBIM). With a strategic focus on bolstering data protection, IdentityCare aligns with the Department of Homeland Security's IT Strategic Plan 2023, specifically targeting Goal 6, which emphasizes enhanced identity verification measures. IdentityCare enjoys a distinct advantage not only with increased speed, accuracy, and spoof resistance of NIR biometric authentication but with intrinsic privacy baked not only into the software but the credential itself.

### **Target Applications**

IdentityCare technology is designed to work with a wide array of devices, operating systems, and services. IdentityCare increased accuracy, 1:N authentication, and the use of asynchronous encryption based upon the distinctiveness of characteristics of the user to protect the enterprise. IdentityCare is FIDO2 compliant, and can be applied to logical access of data via FIDO2 AAGUID architecture, communications, and the content therein such as cell phones, tablets, laptops, desktops, handheld scanners, kiosks, ticketing, Point-of-Sale, ATMs, and other electronic-based devices where secure access is desired.

Rather than merely aspirational, IdentityCare with partner StoneLock has developed licensing kits for indoor applications, FIDO complaint, Application Specific Integrated Circuit (ASIC), and handheld/portable development kits. Before FIDO2 and the application of a SaaS model and containerization for digital attestation, the technology was deployed in the field as a stand-alone product or integrated into an enterprise system, first through a dedicated external control unit and then redesigned with the second generation of the technology to a proprietary gateway software component which acts as a complete biometric-centric credentialing and access control solution. Addressing the need for scalability and versatility in systems integrations, the gateway software delivers a high-performance link between capture devices and external systems capable of providing credentialing data or desiring to monitor activity. The gateway software also provides a seamless integration to six major physical access control (PAC) systems with API's that allow unprecedented connectivity between existing legacy systems, a web client capable of managing the solution from either a PC or mobile device, and the ability to perform analytics on client's data without invoking BIPA requirements pertaining to PII.

The Company can deploy existing biometric capture devices for small scale revenue based on monetizing identities. Hardware adaptation is also available to make the next step for larger scale within the Enterprise. with phone dongle or webcam for the remote capture of the necessary biometric as the identity credential. The Company has also had involved discussions with a computer manufacturer to imbed the necessary hardware that makes the identity credential consumer ready and the first step to making the solution ubiquitous.

Multiplying the adaptability and modularity, IdentityCare technology can utilize the containerized management system within various open-source operating systems (e.g., Amazon BottleRocket, Microsoft Azure, Google Cloud), enabling wireless connectivity, and the deployment of revenue producing applications at the edge. In 2023, IdentityCare migrated existing architecture and code into containers that work to reproduce normal functionality and utilized Amazon BottleRocket to optimize the performance of the containers. The first prototype of the IdentityCare solution was shown to work 3Q23. A Windows version was created for a POC demo of the PC version and demoed to many end-clients in 4Q23.

At its most basic level, the containerized IdentityCare allows the user access through one credential to all applications on the system instead of having to go through standard identification protocols for each application. Revenue may be realized from apps at the door. Revenue may also be enhanced with these applications at the edge providing customized content based upon the credential akin to customized search content and advertising available and based upon activity on the web.

### **Case Study: IdentityCare Deployed with a Bank: What are the Benefits?**

The financial service sector is a focus area for IdentityCare success; however, IdentityCare seeks to first deploy identity management system with a bank or credit union outside the national banks (e.g., Bank of America and JP Morgan Chase) or even regional banks such as (PNC or Huntington Bank). This targeting is two-fold based upon the innovation often found in such smaller financial institutions supported by top-down decision making and deployment of innovation on a smaller scale with less regulatory requirements on the state(s) and federal level.

IdentityCare with its partners would create a modular identity credentialing system that would protect the bank, employees, customers, and financial data from vault to customer's residence. IdentityCare and its partners would protect the bank's premises through physical access control based upon the acquisition of the employee identity. Once captured by the NIR edge devices, the identity may be used throughout the bank enterprise as a 1:N credential with varying degrees of access, security, and privileges. The same modular IdentityCare credential that allows access to the front door would then be for access to one's workstations, computer, data center, bank vault, and any other physical space or asset. The ability to equate such access with a credential based upon identity (because the credential is "something you Know, something you Have, and something you Are") provides lower costs (than badging, HID card, or PIN management) with higher versatility as to access areas, with far greater accuracy and security.

More importantly, the same IdentityCare credential could be used to ensure appropriate access to data, networks, customer information, wiring instructions, bank processes whether on premises or online (e.g., bill payment) from bank work site or remote. As with the premises analysis above, the credential can provide varying levels of access and authorization, but also significantly greater ability for attestation, full audit trail to mitigate risk, and by creating asynchronous encryption based upon the identity credential to ensure that even if the banking network is breached only the recipient with the IdentityCare credential can access the data (as covered by at least the '917 patent above).

Deployment across the bank enterprise accessible by employees would not only significantly reduce fraud based upon stolen credentials, but also decrease the need and cost for hardened systems throughout to protect from cyberactivity. Utilization of the IdentityCare credential and management system would also make it far easier and cheaper to perform those services internally (check processing, brokerage services, mortgage, and other loan processing within requirements of

ECOA, underwriting, and payment, CSR) traditionally provided by third party vendors whose own networks may be susceptible to cyberactivity without the asynchronous encryption based upon the IdentityCare credential. Such a protection is essential because a bank customer does not differentiate between fraud on her Wells Fargo account that was caused by the third party processing her check.

Bank customer experience would similarly benefit from the deployment of IdentityCare at kiosks, ATMs, on-line banking services, debit/credit card processing where the transaction would not be authorized unless the user presented her IdentityCare credential - herself - in person satisfying the requirement for “something she Knows, something she Has, and something she Is”. Additional benefits would include audit trail, risk mitigation, and easing regulatory KYC customer due diligence requirements- all with cost savings, fraud reduction, and opportunity for increased revenue. Deployment of IdentityCare with the SaaS model and containerization makes for much simpler adoption by bank customers.

The enhanced user experience allows for easier adoption by customers (particularly those already accustomed to FaceID and controlling credit/debit cards on one’s smart phone). At a minimum, the bank customer using the identity credential will be able to have one key for all apps (“one key to control all others”) eliminating not only multiple steps in the process but variability within app authentication requirements. Having the ability to provide apps associated with the IdentityCare products provides for customized offers based upon the credential just as offers are now based upon online search history. Finally, there is value in the identity itself for marketing, research and commercial utilization.