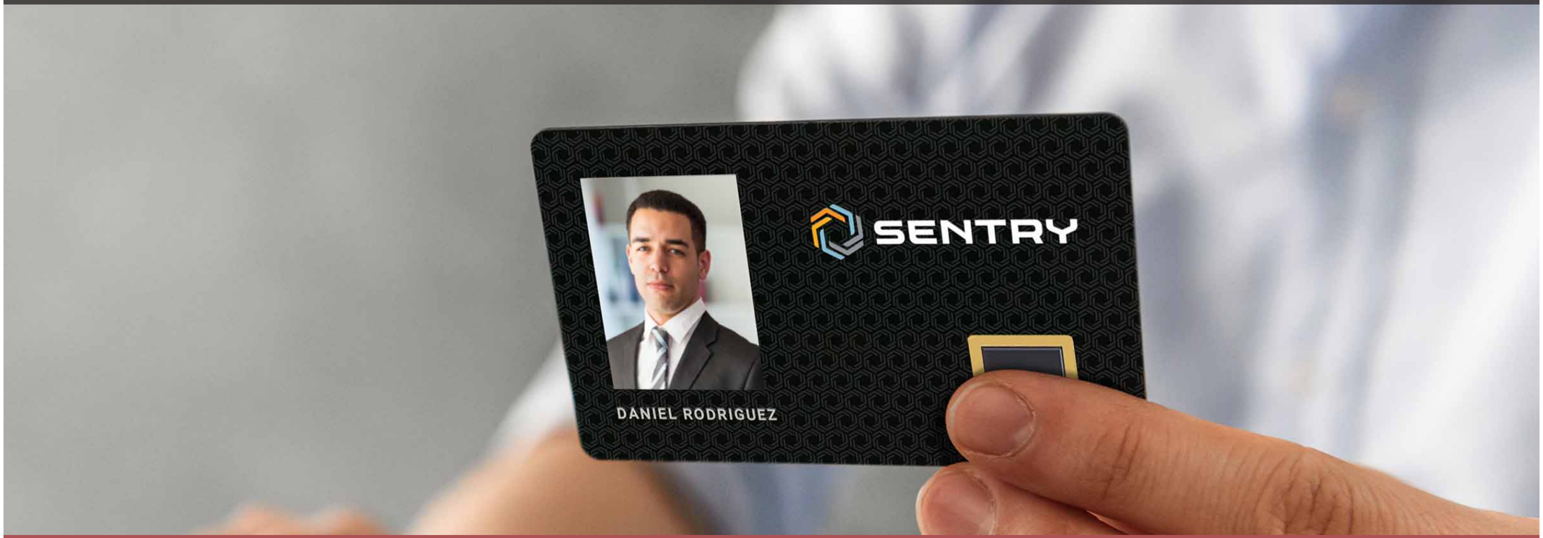
Information Controls

Access Control – SentryCard

INFORMATION CONTROLS INC
Access Control Division



The closest thing to absolute!

SentryCard is a unique, self-contained, biometric platform. This special credential is disconnected from any network, server, or software - making it undiscoverable.

A privacy-driven, leading edge, compatible credential solution.

The biometrics are enrolled, stored, and matched solely within the SentryCard. As a result, broad range privacy concerns are alleviated; including GDPR and BIPA.+ In addition, SentryCard is unphishable standards-based passwordless authentication method.* This credential is compatable with industry leading platforms and readers. As a result, existing infrastructure can be used while phasing in this technology.

KEY PRIVACY CONCERNS: The SentryCard eliminates most of the risks associated with using biometric authentication by removing all human access to the biometric data.

Decentralized	Biometric data is enrolled, stored, and matched solely within the SentryCard platform, never touching an external database or server. With this credential there is no large "honeypot" of biometric data for hackers to pursue.
Unique	Each SentryCard generates its own unique inaccessible encryption key used to protect the biometric data stored within the card.
Non-transferable	The SentryCard is a single-use solution. Once a person's biometrics are enrolled only that person can ever use the credential.
Controlled	Once issued, the holder maintains control of their biometric data, stored securely within the credential.
Irretrievable	Enrollment of the holder's biometrics are one-way and irreversible once set. The credential's only output is an affirmative or negative authentication.

(815) 484-2100 AccessControl@icico.com

Information Controls Divisions

Access Control Human Capital Management Document Imaging Professional Services

+ See https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57 for BIPA information and https://gdpr.eu/ for information on GDPR.

* FIPS 140.0 certification pending.

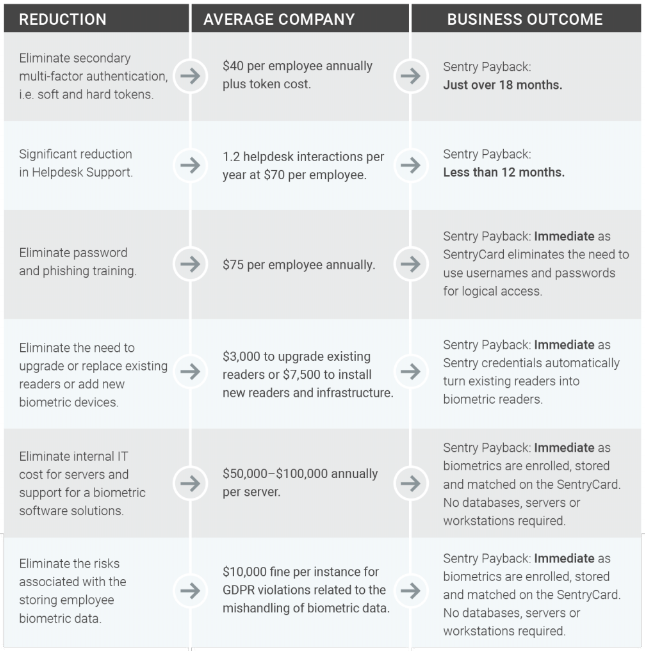
SENTRYCARD WORKS FOR YOUR BUSINESS

Leveraging SentryCard and its multiple use cases

BIOMETRIC PHYSICAL ACCESS

SentryCard can work in conjunction with existing physical access control infrastructure, replacing standalone biometric solutions. SentryCard and its data is undiscoverable until the user is biometrically authenticated, protecting the privacy of the user and the potential lability to the organization.

SO MUCH SAVING WITH SENTRYCARD



REDUCTION		AVERAGE COMPANY		BUSINESS OUTCOME
Eliminate secondary multi-factor authentication, i.e. soft and hard tokens.	→	$40 per employee annually plus token cost.	→	Sentry Payback: **Just over 18 months.**
Significant reduction in Helpdesk Support.	→	1.2 helpdesk interactions per year at $70 per employee.	→	Sentry Payback: **Less than 12 months.**
Eliminate password and phishing training.	→	$75 per employee annually.	→	Sentry Payback: **Immediate** as SentryCard eliminates the need to use usernames and passwords for logical access.
Eliminate the need to upgrade or replace existing readers or add new biometric devices.	→	$3,000 to upgrade existing readers or $7,500 to install new readers and infrastructure.	→	Sentry Payback: **Immediate** as Sentry credentials automatically turn existing readers into biometric readers.
Eliminate internal IT cost for servers and support for a biometric software solutions.	→	$50,000–$100,000 annually per server.	→	Sentry Payback: **Immediate** as biometrics are enrolled, stored and matched on the SentryCard. No databases, servers or workstations required.
Eliminate the risks associated with the storing employee biometric data.	→	$10,000 fine per instance for GDPR violations related to the mishandling of biometric data.	→	Sentry Payback: **Immediate** as biometrics are enrolled, stored and matched on the SentryCard. No databases, servers or workstations required.

> "Utilizing the SentryCard will demonstrate to regulators your commitment to protecting your employee's sensitive biometric information."
>
> David Ross
> Chief Privacy Officer
> GreyCastle Security

For more about BIPA visit
https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57
and https://gdpr.eu/ for information on GDPR.
* FIPS 140.0 certification pending.