



SECURE FINANCIAL SYSTEMS & PERSONAL DATA WITH BIOMETRICS

The Future of User Identity Management

The Need for Biometric Authentication in Financial Services

Data lost to cybercrimes will climb to \$2 trillion by 2019.¹ The average cost of a data breach in the US is over \$7M.²

Data Breaches cause organizations:

- 29% in lost revenue
- 22% in lost customers
- 23% in lost new business³

Most banking customers fear the theft of their bank account information, credit card details, and banking passwords.² Bank fraud and identity theft are banking customers' top concerns — even higher than terrorism.²

Nearly 40% of customers are willing to pay fees for more protection of their banking information. About half the consumers surveyed said they would consider switching to a new bank for greater protection.⁴

81% of data breaches are caused by weak, default, or stolen passwords.⁵ Only multi-modal, multi-factor biometric user authentication verifies the real identity of a person.

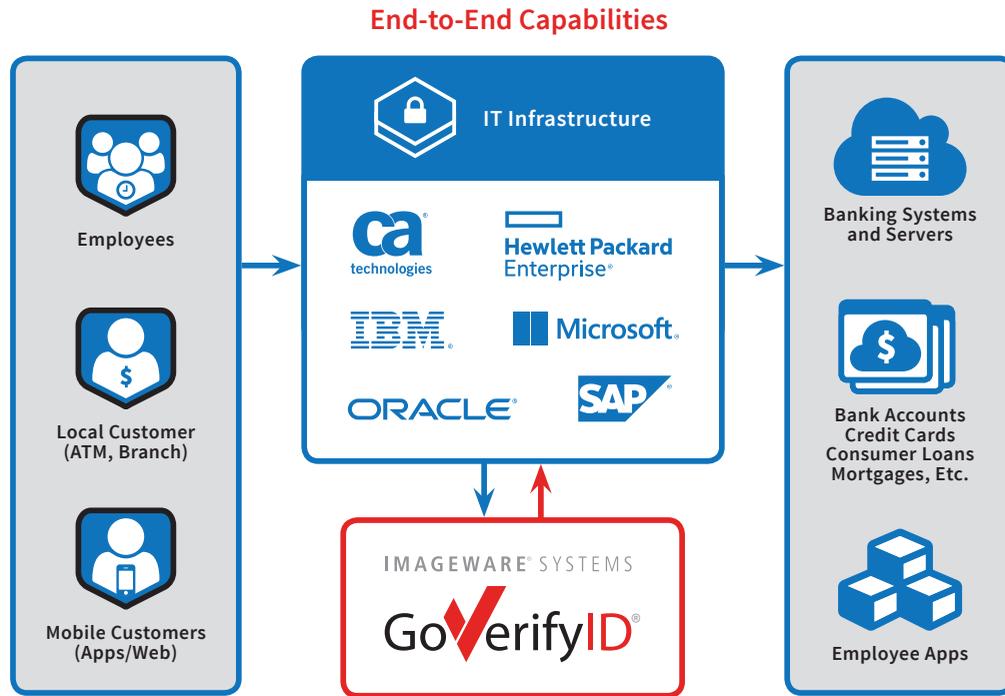


“It takes 20 years to build a reputation and five minutes to ruin it.” —Warren Buffet

1 Cyber Crime Costs Projected to Reach \$2 Trillion by 2016 — <http://bit.ly/2qT0IVX>
 2 2016 Ponemon Cost of Data Breach Study — <http://ibm.co/2pyTlve>
 3 Cisco 2017 Annual Cybersecurity Report — <http://bit.ly/2jtum0w>
 4 Bank customers willing to pay for online security — <http://cnet.co/2g1kXZY>
 5 2017 Data Breach Industry Forecast — <http://bit.ly/2gJqu76>

GoVerifyID Turnkey Solutions for the Financial Services Industry

ImageWare GoVerifyID provides an intuitive user experience for biometric user authentication across all platforms, including Apple iOS, Android, PCs, and other systems. Organizations and users can select the biometrics of their choice, such as face, voice, fingerprint, iris, and palm. Biometric matching can be performed on-device, in the cloud, or on your own servers. GoVerifyID Enterprise Suite provides seamless integration with the security infrastructure that is commonly used in the financial services industry. This includes certified integrations with products from Microsoft, CA, IBM, Oracle, SAP, and HPE.



Workforce Use Cases

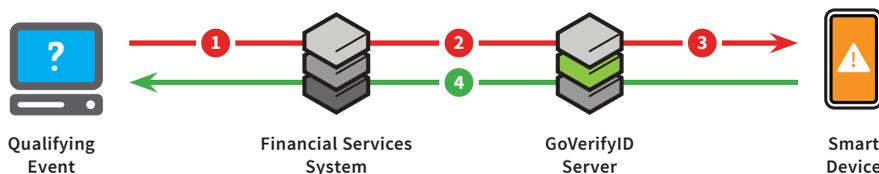
- Computer Access
- Application Access
- Network Access
- Public Cloud Access
- Token Replacement
- Password Reset

Banking Customer Use Cases

- Identity Proofing
- Online Banking
- Mobile Banking
- PIN-free, Card-free ATM
- Transaction Confirmation
- Mitigate Fraud

Mobile Biometric User Authentication: How it Works

- 1 An employee/customer access or verification request starts the process.
- 2 The financial services system contacts the GoVerifyID server with an authentication request.
- 3 The user is asked to submit their biometrics via their PC or mobile device for authentication.
- 4 Depending on the results of the biometric comparison, user access is granted or denied.



For more information, contact us at (858) 673-8600 or sales@iwsinc.com



ImageWare® Systems delivers multi-modal biometric user authentication with patented, agnostic, plug-n-play technology, promoting interactive communication and Out-of-Band (OOB) authentication via mobile devices and in the cloud. Our innovative offering, such as GoVerifyID® and GoMobile Interactive®, provide scalable, reliable, simple, and fast identity solutions across a variety of platforms. ImageWare, GoVerifyID, and GoMobile Interactive are registered trademarks of ImageWare Systems, Inc. © 2017 ImageWare Systems, Inc. All other trademarks are the property of their respective owners. All rights reserved. For more information, please visit www.iwsinc.com