IMAGEWARE® SYSTEMS

GoVerifyID

GoVerifyID Solution Brief

How to secure your assets and provide a convenient login experience.

Executive Summary

Challenges
Data Breaches are one of the leading security concerns for IT organizations. In the majority of cases, compromised passwords are used to gain access to confidential or personal data[1].

Why do we still rely on passwords?

Because they are cheap and easy.[2]

The perceived complexity of implementing biometric technology and concerns regarding user adoption of more complex login procedures, deter organizations from implementing more secure solutions. Even though they are much more secure, biometrics are also perceived as expensive to implement and difficult to adopt.

Solution
ImageWare Systems' GoVerifyID provides unparalleled user authentication assurance while also eliminating the issues regarding implementation complexity, startup costs, and user adoption.

GoVerifyID provides patented multi-modal biometric fusion identity authentication that can be used in place of passwords or as a strong second factor authentication method.

GoVerifyID is provided as a cloud-based Software-as-a-Service (SaaS) solution; thereby, eliminating complex IT deployment of biometric software and eliminating startup costs. GoVerifyID works with your existing mobile devices eliminating the need for specialized biometric scanning devices typically used with most biometric solutions.

Thanks to Apple, Samsung, and other vendors, the use of biometrics on mobile devices has become commonplace. The GoVerifyID mobile app is easy to use, making user adoption a breeze.

BENEFITS

- Unparalleled user identity authentication assurance when using multiple biometrics.
- Flexible enough to work with any business scenario, use-case, existing system, and environmental need.
- Scalable to support hundreds of millions of user identities and transactions in real-time.
- No start-up costs. Pay-as-you-go, SaaS subscription.
- Easy to use, cloud-based, SaaS solution. Simple IT deployment.
- BYOD using your existing personal or corporate mobile devices. No need for new hardware.
- Easy user adoption. As simple as taking a selfie, swiping your finger, and talking to Siri.

[1] Verizon Data Breach Investigations Report - 2014
verizonenterprise.com - www.goo.gl/bwcxPc

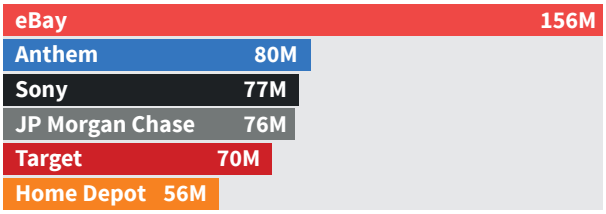
[2] "Why Do We Still Use Passwords?" Government Technology - 2013
govtech.com - www.goo.gl/iuq2IU

Mitigate Data Breach Risks and Provide Convenient User Login

Data Breaches

Data breaches are occurring at an ever-growing and alarming rate, subjecting individuals and corporate data to identity theft and industrial espionage.

RECENT MAJOR DATA/RECORDS BREACHED



KEY IT SECURITY STATISTICS

- Almost 50% of organizations have had at least one data breach.[3]
- According to Experian and IBM research studies, the average data breach costs organizations $3.5 million[3] or $4 million[4] respectively.
- The likelihood for an organization to have a data breach involving 10,000 or more records is estimated at 26% over a 24-month period.[4]
- A Russian crime ring has stolen 1.2 billion usernames and passwords.[5]
- Hackers can crack 16 character passwords in less than 1 hour.[6]
- 63% of confirmed data breaches involved weak, default or stolen passwords.[7]
- Major recent data breaches include eBay (148 million records), Anthem (80 million records including Social Security Numbers), Sony (77 million records), JP Morgan Chase (76 million records), Target (70 million records), Home Depot (56 million records), and many more.[8]
- The leading cause of CIO termination is due to security breaches.[9]
- The top two actions for reducing security risks are implementing 2-factor authentication and patching web servers.[7]

KEY HEALTHCARE INDUSTRY IT SECURITY STATISTICS

- The potential cost of breaches for the healthcare industry could be as much as $6 billion annually.[10]
- The healthcare industry accounted for 42% of the major data breaches reported in 2014.[3]

Shortcomings of Traditional Security Solutions

Passwords and PINs are inadequate security measures as they are often weak, making them subject to guessing and brute force attacks, and are often written down or shared with others; thereby, reducing their security. Passwords are commonly stolen as part of data breaches, users re-use their passwords all too often and users fail to change them even after known data breaches.

Knowledge-Based Authentication (KBA) is a method of authentication that seeks to prove the identity of someone by using private information. Static KBA uses pre-agreed or "shared secrets," such as your favorite sports team or first pet's name. However, these types of so-called "secrets" can often be googled by hackers. Dynamic KBA is based on information that a service provider can determine about your history, such as previous home addresses, phone numbers, etc. If the KBA service provider can find out this information, then hackers can too.

One-Time-Passwords (OTP) provided via email do provide an additional factor of authentication, but they can also be easily comprised if the hacker has access to your email account, which is typical if they already have your primary password.

Second-factor out-of-band security methods, using SMS messaging, can provide an additional security element using a mobile device. This can be easily compromised if the device is lost or stolen. According to the LA Times, 4.5 million smartphones were lost or stolen in the U.S. in 2013.[11]

Token-based security, using Smart Identity Cards or dynamic PIN generating devices, provide additional security. However, if you lose your laptop, you often lose your smartcard or token device too. Dynamic tokens are expensive to buy and replace if they end up in your washing machine. Also, these devices are generally tedious, if not annoying, to use.

More importantly, for all of the security approaches described above, they are not actually identifying the user. They are only validating something the user knows or has in their possession. Only by using biometrics can you really verify the person.

[3] Experian 2015 Data Breach Industry Forecast
experian.com - http://goo.gl/wYKxcQ

[4] Ponemon Cost of Data Breach Study - 2016
ibm.com - www.goo.gl/K77yk9

[5] NBC News - 2014
nbc.com - www.goo.gl/oGLiCB

[6] Daily Mail UK "Think you have a strong Password? Hackers crack 16-characters passwords in less than an hour" - 2013
dailymail.com - www.goo.gl/u1cpX

[7] Verizon Data Breach Investigations Report - 2015 & 2016
verizonenterprise.com - www.goo.gl/bwcxPc

[8] The Huffington Post "The 9 Biggest Data Breaches of All Time" - 2015
huffingtonpost.com - www.goo.gl/TQtWPR

[9] Forbes magazine "Four Reasons Why CIOs Get Fired" - 2013
forbes.com - www.goo.gl/ybQZQa

[10] Ponemon Institute "Sixth Annual Benchmark Study on Patient Privacy & Security of Healthcare Data" - 2016
ponemon.org - https://goo.gl/fUD9QE

[11] LA Times "4.5 million smartphones were lost or stolen in the U.S. in 2013"
latimes.com - www.goo.gl/d4CJgW

IMAGEWARE® SYSTEMS

GoVerifyID®

IMAGEWARE'S MOBILE BIOMETRIC USER AUTHENTICATION SOFTWARE AS A SERVICE

You become the password.

GoVerifyID Overview

ImageWare Systems' GoVerifyID is a mobile biometric authentication solution that is used to verify a user's identity prior to granting access to secured physical or digital sites or to protect transactions. Users enroll their face, fingerprint, and voice biometrics; then use those biometrics much like a password. GoVerifyID works with ImageWare Systems' secure cloud service, to deliver fast, accurate identity authentication that protects all of your important applications, systems, and data such as:

GoVerifyID was built to work seamlessly with ImageWare Systems' patented technology portfolio, including GoMobile Interactive, the secure dynamic messaging system, and the ultra-scalable IWS Biometric Engine that provides anonymous biometric matching and storage. GoVerifyID is secure, simple to use, and designed to provide instant identity authentication by engaging with the biometric capture capabilities of each user's mobile device to:

- Create a baseline biometric characteristics profile
- Store a user's biometric characteristics in the cloud
- Perform two-way messaging communication
- Send customized messages to users
- Perform biometric authentication of a user's identity against their enrolled profile

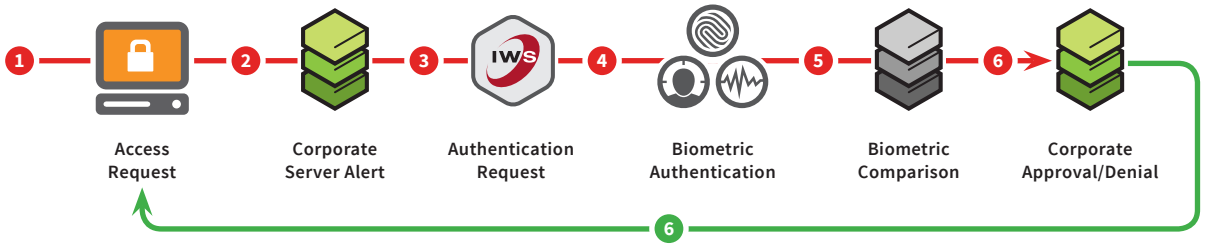
Once the user's biometrics have been captured by the GoVerifyID application, they are transmitted anonymously through our cloud-based, Software-as-a-Service (SaaS) system to the IWS Biometric Engine® database servers for storage and authentication. It is important to note that the actual biometrics (e.g. face picture) are not stored; rather just characteristics of the biometrics are stored.

GoVerifyID is quick-to-implement and an easy-to-use biometric identity authentication SaaS that addresses current security challenges.

GoVerifyID System Workflow

The GoVerifyID SaaS solution uses out-of-band biometric authentication, such as voice or face recognition, to protect secured data and authenticate user identities. Out-of-band means that the user's identity authentication request is sent to the user's mobile device even if they are currently working on their PC. The steps in the GoVerifyID solution workflow are shown below.

1. An individual attempts to access an account or site protected with ImageWare Systems' GoVerifyID SaaS system.
2. The corporate server alerts ImageWare Systems' GoVerifyID SaaS system about this request for access, along with the user's identifier for this request.
3. ImageWare Systems' GoVerifyID SaaS system sends an authentication request message to the GoVerifyID app on the user's mobile device.
4. The user is prompted by the GoVerifyID mobile app to capture their biometrics using the GoVerifyID app on their mobile device.
5. ImageWare Systems' GoVerifyID SaaS server compares the user's biometrics and then returns either an authentication or rejection message back to the corporate server.
6. The corporate server responds to the point-of-origin application, site, or system with an approval or denial of access.



Why biometrics? Why multiple biometrics?

Only biometrics identify an actual person as opposed to just identifying a piece of information or a device. Biometrics can never be forgotten or shared with others. Also, biometrics are difficult to steal as long as the biometric vendor uses appropriate architectures and security methods.

Why perform biometrics in the cloud?

Storing your biometric data on a device might seem secure, but the smartphone vendors' hardware security schemes have already been compromised.[12, 13] Also, you would need to enroll your biometrics on all of your devices and if your devices are lost or stolen, then you have lost your biometric data. By storing your information in the cloud, you can use the same biometrics enrollment for all of your devices – including new or replacement devices that you purchase.

Why GoVerifyID?

ImageWare Systems' GoVerifyID solution provides fast, real-time biometric identity authentication as a cloud service with massive scalability and unparalleled security. Biometric identity authentication can be provided in seconds even with hundreds of millions of identities. The biometric characteristics are stored in a proprietary binary format anonymously. So even if the data is somehow compromised from the secure cloud data center, the data is not usable and it's not associated to any person – so it does not provide any value to a would-be thief.

Only GoVerifyID **provides a secure, scalable, flexible, versatile, mobile and cloud service** for multi-modal biometric identity authentication.

The GoVerifyID mobile app is highly versatile to support any business scenario, environmental situation, use case, application, and system. The GoVerifyID mobile app is a turnkey solution, which can be used without any configuration. The GoVerifyID mobile app can also be easily re-branded to use your company logo and company colors via simple configuration without any programming. The layout and functionality of the GoVerifyID app screens can also be configured using HTML5 or other standard mobile webpage standards. If desired for a completely customized solution or for embedding into your existing mobile application, an open SDK is available for Android and iOS devices.

Why ImageWare Systems?

ImageWare Systems has over 20 years of experience in the biometric identity authentication industry with proven solutions deployed for over 100 major organizations, including the U.S. Department of Justice, the U.S. Federal Bureau of Investigation, the U.S. Veterans Administration, the Canadian Air Transport Security Authority, the Los Angeles World Airports (i.e. LAX, etc.), the Los Angeles Sheriff's Department, the Arizona Department of Public Safety (for DMV and Law Enforcement), the Baja California driver licensing agency, and more.

[12] International Business Times
"iPhone 6 Touch ID Fingerprint Scanner Hacked Days After Launch" - 2014.
ibtimes.co.uk - www.goo.gl/rBjOEi

[13] IT Pro "Hackers can abuse Galaxy S6 fingerprint tech" - 2015
itpro.co.uk - www.goo.gl/CVFbMR

GoVerifyID Use Cases

Many important use cases exist for adding multi-modal biometric identity authentication to business processes within enterprises, the retail industry, the banking industry, and in healthcare organizations. Some of the most obvious use cases are described below. Using GoVerifyID is beneficial any time you need assurance of the identity of the person accessing a system or making a transaction.

ENTERPRISE

1. **Application Access (Direct application login or using Single Sign-On systems)**
   - Includes applications that are hosted on premise or in the Cloud.
   - Often provided in conjunction with a Single Sign-On (SSO) product (e.g. CA Single Sign-On, OneLogin, etc.).
2. **Mobile Device Application and Data Security**
   - Includes securing access to mobile apps and corporate data accessed from mobile devices.
   - Provided in conjunction with a mobile device management product (e.g. MobileIron, Good Technologies, Citrix XenMobile, etc.).
3. **Password Reset**
   - Includes using GoVerifyID to authenticate a user before they can reset their password.
   - Generally provided in conjunction with a password reset vendor (e.g. Avatier, Courion, etc.).
4. **Corporate Network Access**
   - Includes securing access to corporate networks and data using VPN, Firewalls, etc. (e.g. Aruba, Cisco AnyConnect, F5 Networks, etc.).
   - Can replace or supplement token devices, such as RSA SecureID and other products.
5. **Enterprise Data Security**
   - Includes securing access to cloud or hybrid corporate data storage systems (e.g. Box, DropBox, etc.).
   - Recommend using enterprise hybrid storage solutions, like Extenua Cloud2Drive, to provide enterprise security with convenience.
6. **Cloud Access**
   - Login access to public cloud systems, such as AWS, Azure, Force.com, etc.
   - These cloud services provide SAML or other interfaces that can be used with GoVerifyID.
7. **Password Manager Products**
   - Products that securely store all of your passwords in a software vault for access to all of your devices.
   - The security of the password manager product itself is critical since it stores all of your other passwords.
   - Adding GoVerifyID for multi-modal biometric identity authentication to these products is very beneficial.
8. **GPS and Logistic System Integration**
   - When a vehicle or person has to be located via GPS, such as in Logistics and Mobile Health applications.
   - The GoVerifyID multi-modal biometric identity authentication can provide assurance of the user's identity for these types of applications.

HEALTHCARE

1. A physician or other hospital staff requesting access to a patient's electronic health records (EHR) or Personal Health Information (PHI).
2. A physician sharing patient records with other staff within the same health system.
3. Physicians submitting electronic prescriptions (e-Rx) for controlled substances and e-Prescription renewals.
4. Physicians entering orders into Certified Physician Order Entry (CPOE) systems.
5. Patient check-in using biometrics to more easily and accurately identify your patients.
6. Nurses or care workers visiting a patient's home using connected mobile health applications to monitor and track PHI.
7. Physicians' remote access from PC or mobile devices to remote presentations, clinical portals, and shared workstations.
8. Internal password reset requests within hospitals and clinics.
9. Doctors accessing a patient's biographic data (vital signs) from wearable apps and other remote, wireless monitoring devices.
10. Hospitals and clinics offering patient portals to provide remote access to review lab results, Personal Health Information (PHI), and to schedule appointments.
11. Hospitals and clinics providing mobile health applications to communicate, monitor, and support patients.
12. Identifying patients in clinical trials, providing surveys, and collecting patient status during the clinical trial.

RETAIL

1. Login for an online store via a webpage.
2. Login for a mobile store via a mobile device (iOS or Android).
3. Verify a purchase from an online store.
4. Verify a purchase from a mobile store.
5. Point-of-Sale Integration. Verify a purchase made in a physical store.
6. Loyalty programs that send coupons and offers to a mobile phone.

FINANCIAL

1. Login for an online banking website using a PC.
2. Login for a mobile banking app using a mobile device (iOS or Android).
3. Verify a banking transaction from a bank's website.
4. Verify a transaction from a mobile banking app.
5. Verify a transaction performed on an ATM, by using GoVerifyID on a mobile device.
6. Fraud prevention by authorize/decline of unusual transactions via biometric authentication.
7. Authorization of periodical charges/payments (credit card payment, services payment, etc.).

Summary

ImageWare Systems' GoVerifyID provides unparalleled user authentication assurance, while also eliminating the issues regarding implementation complexity, startup costs, and user adoption. GoVerifyID provides patented multi-modal biometric fusion identity authentication that can be used in place of passwords or as a strong second-factor authentication. GoVerifyID works with your existing mobile devices to eliminate new hardware costs for specialized biometric scanning devices. Also, GoVerifyID is provided as a cloud-based SaaS solution; thereby, eliminating complex IT deployment of biometric software and eliminating start-up costs.

Regarding user adoption, the GoVerifyID mobile app is as easy to use as taking a selfie, swiping a finger, or talking to Siri. Taking your own picture, swiping your finger, and/or speaking a passphrase takes less time than entering a complex password, and it's easier and more fun. Also, the GoVerifyID mobile app and SaaS solution is fully configurable to work with your desired applications, systems, use cases, and environmental situations.

Benefits

- Improves security with biometric Multi-Factor Authentication (MFA)
- No more forgotten passwords or lost RSA tokens
- Simple, intuitive, fast with no disruption to workflow
- Allows organizations to fully harness mobile capabilities
- Application does not store Personal Identifiable Information (PII), so your data is safe
- Quick and easy set-up — no coding required
- ImageWare branded or white labeled with fully open SDK

Features

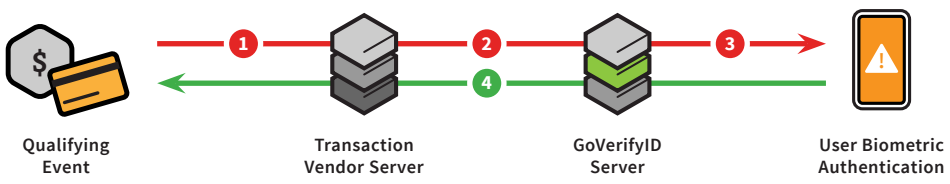
- Highly scalable biometric engine can process hundreds of millions of transactions
- Anonymous cloud storage ensures user privacy and security
- Intelligently combines the matching of multiple biometrics
- Supports all current and future biometric modalities, for in- and out-of-band authentication
- Standard interfaces to SAML, SCIM, and OAuth
- Flexible deployment options
- Available for iOS and Android

Deployment is as easy as 1-2-3

1. Users download GoVerifyID from an app store.
2. A prompt directs users to enroll with their biometrics (face, voice and/or fingerprint).
3. Another prompt directs users to verify their identity with their biometrics. Done.

Mobile biometric user authentication: How it works

1. A qualifying event (like a retail transaction at a store) starts the process.
2. The transaction vendor server (like a bank) pings the GoVerifyID server for an authentication request.
3. The user is asked to submit their biometrics for authentication.
4. Based on the results from the servers, the authentication is approved or denied.



About

ImageWare® Systems, Inc. is a leading developer of mobile and cloud-based identity management solutions, providing biometric secure credential and law enforcement technologies. Scalable for worldwide deployment, ImageWare's patented biometric product line includes a multi-modal Biometric Engine® that is hardware and algorithm independent and enables the enrollment and management of unlimited population sizes. ImageWare's identification products are used to manage and issue secure credentials, including national IDs, passports, driver's licenses, smart cards, and access control credentials. ImageWare's digital booking products provide law enforcement with integrated mug shots, fingerprint live scans, and investigative capabilities.

ImageWare is headquartered in San Diego, CA, with offices in Portland, OR, Washington, D.C., Ottawa, Ontario, and Mexico.

For more information about ImageWare Systems, Inc., please visit **iwsinc.com**

Connect

@iwsinc **linkedin.com/company/imageware-systems-inc** **facebook.com/imagewaresystems**