Think Cloud Compliance

# Secure Biometric Authentication: A Fundamental Building Block for Achieving Trusted Cloud Services

Jeremy Grant
Managing Director,
The Chertoff Group

It has been 23 years since Peter Steiner published the infamous "On the Internet, nobody knows you're a dog" cartoon[1] in The New Yorker, simply and eloquently illustrating the challenges associated with authenticating identity online.

Today, many organizations still struggle to sort out whether people accessing their network information systems are the proverbial "dog on the Internet," meaning that they are who they say they are and are not pretending to be someone else. The consequences of this struggle are significant: year after year, identity continues to be the single most exploited attack vector in cyberspace. The biggest problem? The common password, which has been exploited in breach after breach resulting in significant damage.

*"On the Internet, nobody knows you're a dog."*

The challenge with passwords (and other inadequate authentication methods) only becomes amplified in the cloud. The reason: the rise of cloud, paired with an explosion of mobile devices that connect to it, means that, increasingly, data is being accessed without touching an organization's network, thus bypassing traditional enterprise security controls.  Gartner forecasts that by 2018, 25% of corporate data traffic will bypass the corporate network and flow direct from mobile devices to the cloud.

The implications of this shift are substantial. As the model in which data is accessed changes, so does the importance of the security controls used to protect it. Notably, traditional network security becomes less important, while authentication comes to the forefront.

For this reason, regulators and compliance organizations are increasingly focused on the strength of authentication controls. This paper will:

1. Explore why authentication is so important
2. Discuss barriers to the implementation and uptake of strong authentication solutions
3. Detail the ways in which biometrics and other next-generation authentication technologies are addressing these barriers
4. Lay out key security and privacy risks associated with biometrics, as well as discuss how governments and compliance organizations are framing policies around authentication and biometrics
5. Detail how the right standards and architecture can ensure that biometrics are deployed in a way that addresses important regulatory and compliance concerns

## The Importance of Authentication to Secure, Compliant Cloud Services

In the cloud, the first question any system has to answer is "*are you who you say you are?*" Authentication is the "key" to get in the door to a cloud resource.

The unfortunate frequency of new breaches caused by compromised passwords only increases their focus on the topic. This trend is not waning; as *Table 1* below shows, it is hard to find a major breach over the last few years where weak authentication did not provide the attack vector.

| Breach | Date | Attack Vector |
|---|---|---|
| **Oracle/MICROS** | August 2016 | Compromised Password |
| **DNC** | July 2016 | Compromised Passwords |
| **OPM (2 breaches)** | May 2015 | Compromised Password |
| **Anthem** | February 2015 | Compromised Password |
| **IRS** | May 2015 | Inadequate Authentication (Compromise of "Knowledge-Based" Questions) |
| **JP Morgan Chase** | July 2014 | Compromised Password |
| **Target** | December 2013 | Compromised Password |
| **Apple iCloud** | August 2014 | Compromised Passwords |
| **Home Depot** | September 2014 | Compromised Password |
| **Sony Pictures** | December 2014 | Compromised Password |
| **Heartbleed** | April 2014 | Bug that exposed passwords |
| **1.2 billion passwords (Russian CyberVor hacker gang)** | August 2014 | Multiple – target was passwords to be used for other potential attacks |

*Table 1*

With so many breaches tied to passwords, organizations are not lacking incentives to solve this problem. Breaches like the ones listed in the table above not only result in financial loss, embarrassment, and inconvenience, but many also led to civil penalties stemming from violations of various government regulations and compliance requirements.

- In 2013, WellPoint was fined $1.7 by the U.S. Department of Health and Human Service's Office for Civil Rights for a 2010 database breach stemming from compromised user credentials.[2]
- Following a 2013 breach, Target Corporation was subject to investigations by the U.S. Federal Trade Commission (FTC), U.S. Securities and Exchange Commission (SEC), and state regulatory authorities.[3]
- The Securities and Exchange Commission (SEC) is currently considering an investigation of Yahoo for disclosure violations related to the 2016 breach of user credentials.[4]

The breadth and impact of these civil penalties will only increase in coming years, as new data protection requirements and increased civil penalties come into effect. For example, the European Union's General Data Protection Regulation, which takes effect in May 2018, includes increased penalties for data protection violations, allowing European Data Protection Authorities to levy fines of up to 20 million Euros or 4% of global annual turnover, whichever is greater. The increased penalties, which will be accompanied by additional data protection requirements, make clear the risks facing companies that fail to adequately protect themselves from a breach

Despite the threat of regulatory enforcement, many organizations have resisted implementing stronger authentication due to the inadequacy of first-generation digital authentication solutions.

A key challenge with these first-generation authentication solutions is that they require user to "break stride" to log in – forcing them to not only enter a password, but then find another device – such as a mobile phone or hardware token – read a randomly-generated code off of it, and enter that code into an application. These sorts of solutions degrade the user experience, and as a result, have failed to win fans or gain widespread user adoption.

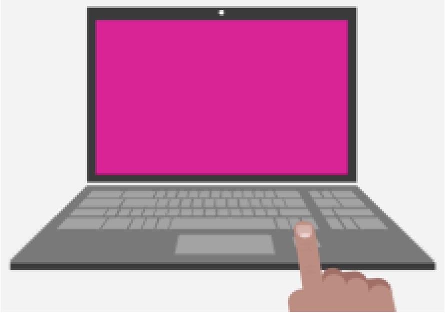
As Table 1 makes painfully clear, despite overwhelming evidence that passwords alone are an inadequate form of security that presents material risks, many enterprises and users have rejected the use of stronger authentication solutions.

This lack of adoption sends a clear message: to get true uptake in the marketplace – and thus enable more trusted cloud services – a multi-factor authentication solution has to not only be more secure than passwords, it must also be easier to use.

> "… despite overwhelming evidence that passwords alone are an inadequate form of security that presents material risks, many enterprises and users have rejected the use of stronger authentication solutions."

## The Promise of Biometrics

The emergence of reliable, easy to use, consumer-grade biometric technologies has fueled significant innovation in the security and usability of authentication solutions, making it easier for organizations to comply with requirements for authentication. Ten years ago, biometrics required expensive, specialized, stand-alone hardware, and its deployment was largely limited to high security facilities. Today, however, most devices ship with cameras and finger sensors that can be used to complement, or in some cases even replace, passwords with fingerprint or face recognition.



Apple's 2013 launch of Touch ID – which gives users the option of unlocking their phones with their fingerprints rather than a PIN – established fingerprint recognition as a widespread, commercial smartphone security offering. Today, fingerprint sensors are a de facto standard offering on smartphones and laptops, and face recognition is also gaining ground. Beyond face and finger, iris, voice, and heartbeat are three other biometric modalities getting traction in the marketplace. Apple has been joined by major manufacturers including Microsoft, Lenovo, Samsung, LG, and Fujitsu in embedding biometric sensors in devices.

From an authentication standpoint, the implications of the consumerization of biometrics are significant: rather than require a user to enter a password or insert a token, biometrics enable a device to simply "recognize" a user. When properly implemented, this can lead to passwordless authentication experiences that are much easier to use, relative to other technologies.

In the cloud – where users expect instant, on-demand access to applications and data – biometrics offer the ability to simplify authentication while also enhancing privacy and security.  Biometrics are helping industry overcome the usability limitations that hindered uptake of first-generation authentication, driving higher adoption of secure authentication tools across the market.

However, all biometrics are not the same – and some technologies and configurations may create significant security and privacy risks, as well as compliance and regulatory challenges. These risks must be addressed in order to deploy biometrics in a responsible, secure fashion that addresses regulatory and compliance concerns.

At the core of this issue is the reality that biometric technologies vary in two key ways:

*First*, some are more reliable than others. Within different modalities – face, fingerprint, and iris being the most common – the market is diverse, with some solutions that are highly reliable and others that are volatile.

Key issues that impact reliability include:

- What is the False Accept Rate (FAR) of the biometric? Meaning, how frequently does the biometric system accept the biometric of the wrong person?
- What is the False Reject Rate (FRR) of the biometric? Meaning, how frequently does the biometric system reject the biometric of the right person?
- Does the biometric sensor incorporate "liveness detection" to validate that the biometric being presented is real?
- Is the sensor adversely impacted by external factors, such as light or moisture?

These considerations, in addition to cost, degree of intrusiveness, storage space, and computing power required, help inform which specific biometric authentication solutions may be appropriate for a specific use case.

*Second*, the various ways in which biometric systems are architected and deployed can have a material impact on whether they enhance security and privacy or detract from it.

One important difference between biometric modalities and other authentication solutions is that other technologies, such as passwords and tokens, can be changed or revoked, meaning that if they are stolen or compromised, there is an easy way to issue someone a new solution.

Biometrics, in contrast, are permanent. Unintended disclosure of biometric data may therefore have consequences that are more difficult to remediate than a breached password.

For this reason, any implementation of biometrics needs to be architected very carefully to mitigate the possibility that someone's fingerprint or face could be compromised.

## Seven Questions to Ask when Implementing Biometric Authentication

How do you determine if a biometric security offering is going to enhance security and privacy or detract from it? For those seeking biometric solutions, it is important to understand the key issues around biometric solution architecture that need to be addressed in order to ensure the highest levels of security, privacy, and performance. Here are seven questions to ask:

1. *Where are biometrics stored? Will the system create a central database of biometric information?*

   Some biometric authentication systems are architected to store biometrics locally; others are designed to store them in central databases. There are also hybrid systems, where biometrics may be stored in multiple places.

   While it may be tempting to store biometrics centrally, databases of biometric information come with some risk, as these databases then become targets themselves, threatening both the integrity of the system, as well as the security and privacy of the people whose data is being stored. The 2015 breach of the U.S. government's Office of Personnel Management (OPM) is an example of the risk created by storing biometrics in a central database; more than 5.6 million people had their fingerprints stolen.[5]

   As noted, one challenge with biometrics is that they are not a secret. Unlike passwords or security tokens, once stolen, they can never be revoked or replaced. For this reason, the risks involved with the compromise of a central biometric data store – even in the cloud – is quite high.

   In contrast, authentication solutions that limit storage of biometrics to the device that they are collected on mitigates the risk of scalable attacks, in that any successful attack generally requires that the attacker gains physical possession of the device. As we detail below, the best biometric implementations make it physically impossible to export biometric information outside of a device. For this reason, it is best practice to ensure that biometrics are protected on devices by storing them in a protected container that is isolated from the rest of the device, or in trusted hardware, such as a Trusted Platform Module (TPM) chip.

2. *Where are biometrics matched?*

   Similar to storage, some biometric systems match the biometric centrally; others only perform the match on the device, and still others embrace hybrid architectures, offering service providers the ability to match through multiple approaches.

   As with storage, central matching systems introduce additional risks around security and privacy, as they mean that biometrics must be exported from a device and transmitted to the central matching location in a secure manner.

   Moreover, central matching systems present privacy concerns, as they can make it easier for an entity to track someone with their biometric over time.

Finally, central matching systems may present performance issues, given the requirement to have network access in order to perform a match.

Local biometric matching systems, in contrast, restrict the transmission of biometric information. They also offer the ability to use biometrics when a system is offline.

3. *Are biometrics the only factor required to get access?*
   Some biometric solutions support only single-factor authentication, with the biometric being the only factor needed to access a system. Other deployments use biometric as just one layer of a multi-factor authentication solution. For example, Microsoft's Windows Hello system – like all biometric solutions designed to meet FIDO Alliance standards – uses the biometric only as an initial factor to then unlock a second factor, in this case a private cryptographic key that is used to authenticate to a system through public key cryptography.

   Given the issues already described with stolen biometrics, as well as the risks that an adversary may look to spoof a biometric system, it is best to use biometrics as simply one layer of a multi-factor authentication solution.

4. *When biometrics are captured, does the solution store the raw images or only store templates?*
   Biometrics are generally stored in one of two formats: either as raw images, much as the U.S. government did in the OPM database that was breached, or as templates that are a mathematical "abstract" of the biometric, but that can be effectively used to match a biometric.

   The advantages of template-based systems are that the templates cannot generally be reverse-engineered if compromised, greatly mitigating the risk to the consumer if biometric information is breached.

   Template-based systems also generally offer superior performance, as the templates are optimized for applications that match biometrics on devices.

5. *How is biometric information protected?*
   Whether stored locally or centrally, biometric information needs to be protected. Any device holding biometric information will be a target for adversaries if there are not layers of protection to prevent an adversary from extracting the biometric data and using it for other purposes.

   Best practices for protection of biometric data include:

   - Storing the biometric as a template, not an image – ensuring that the image cannot be reverse-engineered if biometric information is somehow compromised.
   - Encrypting the template, so that if stolen, the data cannot be deciphered.
   - Storing the template only on the device, not in a central database. Ideally, the template should be stored and matched in a protected, isolated environment in the device, such as one using Virtual Secure Mode (VSM), or in hardware-based security solutions such as a Trusted Platform Module (TPM) chip or Trusted Execution Environment (TEE) that is highly resistant to tampering.

6. *Can biometrics be used to track people across multiple sites or applications?*
   A longstanding concern about biometrics is that they could be used to track the movements, activities, or behaviors of individuals across different applications or locations.

   While there are no shortage of science fiction films that portray biometrics being used in this fashion, the fact is that biometrics that track people do so because of a conscious design choice in the architecture of the solution – not because of anything inherent in biometric technology itself.

   Ideally, biometric solutions are architected in a way to ensure that there is no way to link the use of biometrics between services or accounts, precluding tracking. Limiting storage of biometrics to on-device only is one way to mitigate the risk of tracking.

7. *How easily can an adversary spoof a biometric to access the system?*
   Even the most secure biometric access system may be a target of attack, with adversaries seeking to exploit any attack vector possible in order to compromise a system. A common attack method involves trying to spoof a person's body part, with the goal of tricking the system into thinking that a fake is real.

   The impact of spoofing attacks can be greatly mitigated by architecting biometric access systems in accordance with the ideas laid out above. Most notably, decisions to only store biometrics locally, and in protected areas of a device, make it impossible for any adversary to launch a scalable attack on a broad biometric system; any spoofing attack would first require that the attacker gains custody of the device.

   Beyond these layers of protection, many biometric systems today are building in "liveness detection" to validate that a biometric being presented is in fact real. If there is a risk of a spoofing attack, organizations should take time to understand all aspects of an authentication system, including the ways it might protect against the risk of a spoofing attack.

> “… decisions to only store biometrics locally, and in protected areas of a device, make it impossible for any adversary to launch a scalable attack on a broad biometric system.”

# Biometric Regulatory and Compliance Concerns: Where do Governments Stand?

There are a number of security and privacy risks involving biometric authentication; however, these risks can be mitigated by implementing appropriate technical architectures, standards, and controls that address the seven questions above.

This is not just a technical issue; there are a number of laws, policies, and regulations across the globe that impact the way security, privacy, and data protections apply to authentication systems, and heavily influence the architectures of these systems.

Early adopters of guidance on biometrics, including the European Union, Switzerland, Canada, the United States, Australia, Japan, and Singapore, consider biometric data to be a form of personal—if not sensitive personal—data, and thus hold it to a standard of privacy protection typically afforded to social security numbers, medical records, financial information, and employment history.

- The recently-adopted **European General Data Protection Regulation (GDPR**), for example, specifically calls out biometric data as a subset of sensitive personal data, and places protections on the export of such data outside the EU.[6]
- The United States' **National Institute of Standards and Technology (NIST)** similarly affords "fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry)" the status of sensitive personal information in its Special Publication 800-122.

Putting biometric data on par with other long-accepted forms of Personally Identifiable Information (PII) makes the application of globally accepted privacy principles—such as transparency, individual choice and control, and security and confidentiality—a useful framework through which to consider biometric privacy policy.

- **Transparency**. Jurisdictions including the EU and Australia have addressed the need for transparency by requiring individuals to be expressly informed of who is collecting their biometric data, why that data is being collected, how that data will be used, where it will be stored, and who will have access to it.[7]
- **Individual choice** typically refers to the requirement that freely-given consent be required before biometric data can be captured. While the means of securing consent may vary, the requirement that consent be informed—that a subject be made aware of the various uses for his or her biometric data—is constant.
- **Security and confidentiality** are fundamental to any data privacy policy. Given that many jurisdictions now consider biometric data to be a form of sensitive personal information, security measures must be in place to prevent unauthorized access to such data—as they would be in an organization handling sensitive medical or financial information.

A number of policies across the globe impact the way security, privacy and data protections apply to authentication systems – and point to locally stored, locally matched biometrics as the preferred solution to comply with these policies. Examples include:

- **Switzerland**, where the government has prohibited general consent covering multiple transnational data transfers, set forth policies requiring that data subject consent is required for each instance of international data transfer. This requirement places heavy burdens on central biometric storage systems, which transfer information to and from multiple locations and require organizations to be mindful of any government prohibitions on cross-border data transfer.[8]
- **Canada**, where the **Office of the Privacy Commissioner of Canada** states in its biometric data handling guidance that "centralized storage of biometric data heightens the risk of data loss or the inappropriate cross-linking of data across systems." Instead, the Office advocates one-to-one matching to reduce the risk of false matches.[9]
- **Europe**, where the EU similarly advises against the centralized storage of biometric data. The EU's **Article 29 Working Party** on biometric data advises that "whenever it is permitted to process biometric data, it is preferable to avoid the storage of the personal biometric information." One-to-one, on-device matching accomplishes this while preserving all the security and usability benefits of biometric authentication.[10]

Beyond biometrics, a number of governments have put forth policies requiring the use of multi-factor authentication (MFA) for many applications:

- In the **United States**, Executive Order 13681 – issued in October 2014 – required "all agencies making personal data accessible to citizens through digital applications require the use of multiple factors of authentication and an effective identity proofing process." While biometric authentication is not specifically called out, the new *Digital Authentication Guidance* published by NIST to support this Executive Order (NIST SP 800-63-3) recognizes biometrics as one factor that can be used in a MFA solution.[11]
- Also in the United States, the **Federal Financial Institutions Examination Council (FFIEC)** published guidance requiring use of MFA for a variety of applications across financial services.[12]
- The U.S. **Federal Trade Commission** (FTC) has recommended that businesses use two-factor authentication to protect against password compromises, noting that it has brought enforcement actions against several companies who failed to implement adequate authentication controls.[13] Note that the FTC has also flagged the privacy and security risks with facial recognition biometrics, recommending best practices that include privacy by design, consumer choice and transparency.[14]
- Likewise in **Europe**, the European Union has mandated strong customer authentication under the Payment Services Directive 2 (PSD2). **The European Banking Authority (EBA)** published draft standards in 2016 calling for use of MFA in payments and highlights MFA solutions using biometrics, paired with a second factor, as an example of the type of solutions that will be permitted.[15]
- In **Asia**, the **Hong Kong Monetary Authority** updated its *Supervisory Policy Manual for Risk Management of E-Banking* in 2015, stating "two-factor authentication should be implemented for e-banking channels that allow high-risk transactions" and flagging biometric identifiers as one appropriate second factor.[16]
- In **Australia**, the **Department of Defence** lists MFA as a key tool to be used in its *Strategies to Mitigate Targeted Cyber Intrusions*, noting that MFA "helps to prevent cyber adversaries from propagating throughout an organisation's network" and that it "can make it significantly more difficult for cyber adversaries to steal legitimate credentials to facilitate further malicious activities on the network."[17]

While this is only a sampling of the rules and requirements emerging, the trend is clear:

Regulators understand that strong authentication is essential, that passwords aren't good enough, and that authentication solutions need to be designed to enhance privacy and security, not detract from it.

Beyond regulators, security compliance organizations are also starting to require strong authentication. For example, the Payment Card Industry Security Standards Council (PCI SSC) in its latest Data Security Standard (DSS), v3.2 added a requirement for MFA for any personnel with administrative access to environments that handle payment card data.[18]

The addition of requirements from both regulators and compliance organizations adds a new dimension to potential breaches that occur as a result of poor

> "Regulators understand that strong authentication is essential, that passwords aren't good enough, and that authentication solutions need to be designed to enhance privacy and security, not detract from it."

authentication, adding clear compliance risk to the financial and reputational risks inherent in cyber breaches.

While there are still some instances where regulators have yet to incorporate MFA into their requirements, companies would be well served to start considering their authentication approach, positioning to meet future regulatory requirements while bolstering their own cybersecurity and reducing the risk of a breach.

## FIDO and Windows Hello: a standards-based implementation of best practices for biometric authentication to the cloud

Amidst the technical and regulatory churn, there is good news. New standards have emerged that are focused on addressing security and privacy risks in authentication systems. Microsoft, along with other companies across many different sectors, has been at the forefront of these efforts, and has made it a priority to “bake in” next generation authentication solutions across Microsoft products.

Chief among these authentication standards are the ones crafted by the **Fast Identity Online (FIDO) Alliance** – a consortium of more than 250 members across the globe, including Microsoft, Google, PayPal, several major banks and of security vendors.

The FIDO Alliance was founded in 2013 with a mission to change the nature of online authentication by developing open, interoperable specifications to supplant passwords and other first-generation authentication technologies with new solutions offering more security, privacy and usability. Addressing flaws in legacy authentication solutions, one of FIDO’s principal goals is to achieve a superior user experience by letting people using the same authentication solution across multiple services.

In a typical deployment of these standards, a user swipes a finger, speaks a phrase, or looks at a camera on a device to login, pay for an item, or use another service. Behind the scenes on that device, the biometric is used as an initial factor to then unlock a second, more secure factor: a private cryptographic key that works “behind the scenes” to authenticate a user to the service. Since biometrics and cryptographic keys are stored on local devices and never sent across the network, user credentials are secure even if service providers get hacked, thereby eliminating the possibility of scalable data breaches.

FIDO and its member companies have worked to specifically answer the “seven questions” described above and ensure that strong, biometric-based cloud authentication can be deployed while fully complying with the policies and regulations that different countries have created around the use of biometrics in authentication.

The FIDO approach has been embraced by the World Wide Web Consortium (W3C), who is expected to finalize a formal new “Web Authentication” standard built on FIDO specifications in February 2017. The emergence of this new standard, combined with the wide industry and government support of the growing FIDO ecosystem, makes it likely that regulators will start to point to FIDO in upcoming rules.

Indeed, governments are already pointing to FIDO:

- In the **United Kingdom**, the new UK National Cyber Security Strategy specifically flags the importance of authentication, committing the UK to "invest in technologies like Trusted Platform Modules (TPM) and emerging industry standards such as Fast IDentity Online (FIDO), which do not rely on passwords for user authentication, but use the machine and other devices in the user's possession to authenticate."  The UK strategy noted the need in authentication to address both security, as well as enhanced user experience. [19]
- In the **United States**, new *Digital Authentication Guidance* published by NIST (NIST SP 800-63-3) recognizes FIDO solutions at the highest Authenticator Assurance Level (AAL), given its combination of biometrics and public key cryptography.[20] In addition, the White House Commission on Enhancing National Cybersecurity called out the need for "open-source standards and specifications like those developed by the Fast IDentity Online (FIDO) Alliance" as an example of "important work that must be undertaken to overcome identity authentication challenges," and noting that FIDO "provides a strong foundation for opt-in identity management for the digital infrastructure."[21]

Microsoft has been at the forefront of FIDO, having built the latest set of FIDO authentication standards into Windows 10 through the "Windows Hello" feature. Other major deployments of FIDO include those by Google, Salesforce, eBay, NTT DoCoMo, PayPal, Bank of America, Baidu, BC Card (in Korea), Dropbox and GitHub. Together these firms and others are accelerating the adoption of strong, biometric-enabled cloud authentication solutions that address compliance and regulatory concerns out of the box.

Windows Hello enables users to easily log into Microsoft cloud services today, without a password. Instead, Windows Hello leverages a combination of biometric (either face or fingerprint) and public key cryptography to quickly and securely authenticate to the cloud.

In addition to leveraging biometric authentication to Microsoft services, Windows Hello can also be leveraged by other online service providers such as banks, government, health providers and retailers to ensure their customers enjoy the same secure, passwordless experience to log in to their cloud-based services.

For an added layer of security, all biometric identifiers used in Windows 10 are device-specific. The biometric data used to support Windows Hello is stored on the local device only. It does not roam between devices, nor is it shared with a server or easily extractable from a device. This separation thwarts attackers by eliminating any single point of collection that could be compromised. Even if an attacker were to compromise biometric data, the data is encrypted such that it cannot be converted to a form recognizable by the biometric sensor.

# How do FIDO and Windows Hello answer the "Seven Key Questions?"

| **Question** | **FIDO/Windows Hello Approach** |
|---|---|
| *Where are biometrics stored? Will a system create any new central database of biometric information?* | Biometrics are only stored locally, on-device. There is no central database of biometric information. |
| *Where are biometrics matched?* | Biometrics are only matched locally, on-device.<br>Server-side matches are not supported. FIDO specifications prohibit them. |
| *Are biometrics the only factor required to get access?* | Biometrics are one factor of a Multi-Factor Authentication (MFA) solution. Windows Hello leverages biometrics as the initial factor to then unlock a private cryptographic key stored only in the device. |
| *When biometrics are captured, are the raw images stored, or are they only templates?* | Biometrics are only stored in templates. There are no images to steal; templates cannot be reverse-engineered to extract an image in the event of a compromise. |
| *How is biometric information protected?* | Biometrics are only stored on device.<br>Windows Hello can store biometrics in an isolated environment on the device that offers additional layers of protection. |
| *Can biometrics be used to track people across multiple sites or applications?* | Biometric information is never shared with service providers or permitted to leave a user's device.<br>Moreover, biometrics are used as the initial factor to then unlock a private cryptographic key stored only in the device that is used to sign a corresponding public key stored by the application.<br>A new key-pair is generated for each application where Windows Hello is used. There is no linkability or tracking possible. |
| *How easily can an adversary spoof a biometric to access the system?* | Compromise of the system requires that an adversary obtains the device itself. This precludes the possibility of an adversary executing a scalable attack against multiple devices. |

# Conclusion

Former U.S. Department of Homeland Security Michael Chertoff recently stated, "The password is by far the weakest link in cybersecurity today."[22] Addressing this weakness must be at the top of any effort to mitigate cyber risk, both in the cloud or in legacy on-premise environments.

To truly mitigate cyber risk, meet compliance and regulatory requirements, and realize the full benefits of cloud computing requires a secure login experience that protects against security threats, delights users and protects their privacy. The incorporation of biometrics in the cloud authentication process, when implemented properly and in accordance with industry standards and best practices such as those from the FIDO Alliance, can allow companies to migrate to the cloud in a secure, compliant manner that minimizes inconvenience for users. Doing so also allows companies to avoid the need to devote significant resources to building new systems that meet compliance requirements for authentication, and can instead utilize cloud platforms that have already implemented industry best practices and standards that ensure that they meet their compliance requirements. By adopting a cloud platform that adheres to such requirements and industry best practices, companies can minimize their compliance costs while providing users with a more secure and less frustrating user experience.

No technology or solution can completely eliminate the risk of a cyberattack, but adoption of biometric-enabled, multifactor authentication is one of the most impactful steps that can meaningfully reduce a company's cyber risk. Given the emerging array of new requirements for authentication in sectors such as health, financial services and government, organizations can prepare for cloud compliance by moving to implement MFA now.

## About The Chertoff Group

This white paper was prepared by The Chertoff Group for Microsoft. The Chertoff Group is a premier global advisory firm focused exclusively on security and risk management. The Chertoff Group helps clients grow and secure their enterprise through business strategy, mergers and acquisitions and risk management services. Headquartered in Washington D.C., the firm maintains offices in Houston, London, Menlo Park and New York. For more information about The Chertoff Group, visit www.chertoffgroup.com.

# Notes

[1] Peter Steiner, *The New Yorker*, © Condé Nast. Used under license.

[2] See "WellPoint to Pay $1.7M Over Alleged HIPAA Violations," *Beckers Hospital Review* at http://www.beckershospitalreview.com/legal-regulatory-issues/wellpoint-to-pay-1-7m-over-alleged-hipaa-violations.html

[3] See "Hacked Companies Face SEC Scrutiny Over Disclosure," *Bloomberg*, at https://www.bloomberg.com/news/articles/2014-07-02/hacked-companies-face-sec-scrutiny-over-disclosure

[4] See "Senator calls for SEC investigation into Yahoo breach," *TechCrunch*, at https://techcrunch.com/2016/09/26/senator-calls-for-sec-investigation-into-yahoo-breach/

[5] See Andrea Peterson, "OPM says 5.6 million fingerprints stolen in cyberattack, five times as many as previously thought," *The Washington Post*, September 23, 2015 at https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/

[6] See the European Data Protection Regulation at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[7] See the European Data Protection Regulation and the Australian Privacy Principles at https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/

[8] See the Swiss Federal Data Protection and Information Commissioner's Legal Framework Overview at https://www.edoeb.admin.ch/org/00129/index.html?lang=en

[9] See the Office of the Privacy Commissioner of Canada's overview of Biometrics and the Challenges to Privacy at https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/gd_bio_201102/?wbdisable=true

[10] See the Article 29 Working Party's Opinion regarding Development in Biometric Technologies at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

[11] See Executive Order 13681 at https://www.whitehouse.gov/the-press-office/2014/10/17/executive-order-improving-security-consumer-financial-transactions and NIST Special Publication 800-63-3 at https://pages.nist.gov/800-63-3/

[12] See the Federal Financial Institutions Examination Council's Supplement to Authentication in an Internet Banking Environment at https://www.ffiec.gov/pdf/auth-its-final%206-22-11%20(ffiec%20formated).pdf

[13] See the Federal Trade Commission's "Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies" at https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business

[14] See the Federal Trade Commission's "Start with Security: A Guide for Business" at https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf

[15] See the Directive 2015/2366 of the European Parliament and Council on Payment Services in the Internal Market at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366

[16] See the Hong Kong Monetary Authority's Supervisory Policy Manual at http://www.hkma.gov.hk/eng/key-functions/banking-stability/supervisory-policy-manual.shtml

[17] See Australia's Strategies to Mitigate Targeted Cyber Intrusions at http://www.asd.gov.au/infosec/top-mitigations/mitigations-2014-details.htm#11

[18] See "PCI Standard Adds Multi-Factor Authentication Requirements," *Infosecurity Magazine*, at http://www.infosecurity-magazine.com/news/pci-standard-adds-multifactor/

[19] See the UK National Cyber Security Strategy at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

[20] See NIST Special Publication 800-63-3 at https://pages.nist.gov/800-63-3/

[21] See Report on Securing and Growing the Digital Economy from the White House Commission on Enhancing National Cybersecurity at https://www.whitehouse.gov/sites/default/files/docs/cybersecurity_report.pdf

[22] See Michael Chertoff, "Passwords are the weakest link in cybersecurity today," *CNBC*, http://www.cnbc.com/2016/10/06/passwords-are-the-weakest-link-in-cybersecurity-today-michael-chertoff-commentary.html