FOUR BARRIERS TO ADOPTING STRONG AUTHENTICATION

Any device.
Any application.
Any authenticator.

Nok Nok
LABS

REFRAMING THE PROBLEM OF ONLINE AUTHENTICATION

Authentication is the front door that protects access to everything of value on an Internet provider's network. For a cybercriminal, online authentication is the main obstacle to stealing sensitive customer data – with sensitive information regarding bank accounts and other assets that these hackers can monetize on the dark web. The use of passwords is the weakest security for authentication, yet Internet services providers persist in making consumers use a password as the primary method for access. This whitepaper examines why these Internet services providers have had problems in adopting stronger authentication.

Passwords have severe vulnerabilities. For consumers, there are too many to remember,[1] they are difficult to type on mobile devices,[2] and they are insecure.[3] Despite this, when a provider asks a user – Do you want to login? Do you want to transfer $100 to Joe? Do you want to ship to a new address? Do you want to delete all of your emails? Do you want to share your medical record? – the only authentication method offered is the creation of another password.

There are more secure authentication options that require users to submit one or two extra "factors," which may be any combination of something a user (i) knows, (ii) has, or (iii) is – the classic definition of multifactor or strong authentication ("MFA" or "SA"). These factors provide better protection, yet the nearly universal reason against adopting them is: "Strong authentication has too many barriers." [4]

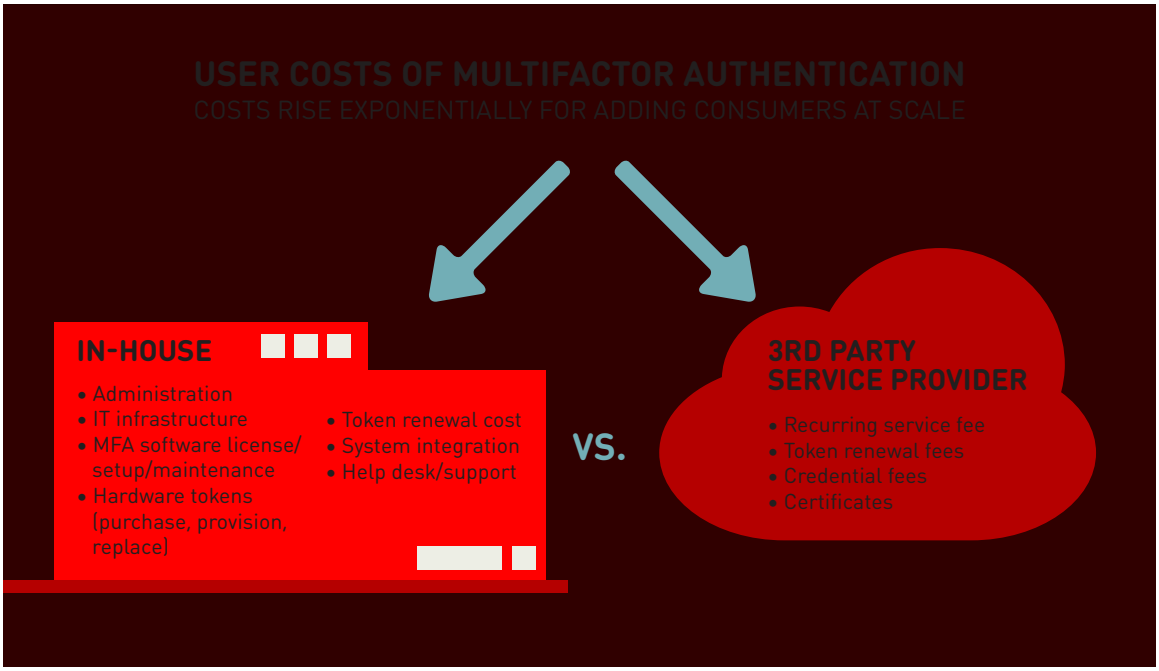
This paper will describe four major barriers to the use of strong authentication: Cost, Usability, Security, and Privacy ("CUSP"). Each of these barriers can carry significant burdens when an organization seeks to adopt strong authentication, and businesses need to consider how these barriers may affect their adoption and deployment of additional authentication capabilities.

At Nok Nok Labs, we, together with our partners in the FIDO Alliance, are deeply engaged in offering technical protocols that help Internet services providers easily remove the 'CUSP' barriers to strong authentication. By using FIDO protocols to easily interconnect the components and methods for strong authentication, providers and other stakeholders will be able to strongly authenticate their millions of consumers in a way that is cost effective, usable, secure, and maintains privacy.

BARRIER 1: COST

Cost is a major barrier to using traditional strong authentication solutions for consumer applications. For a single provider, the business problem requires authenticating a mass audience with heterogeneous devices – potentially millions of customers with diverse PCs, smartphones and tablets – so the cost at scale is often prohibitive. Total cost of ownership for strong authentication is akin to owning a boat (or in this case, a yacht). The acquisition cost is just the beginning of a lifecycle of financial commitments. Even for a cloud-based solution that boasts a lower up-front cost, recurring expenditures during its lifecycle can quadruple the total cost of ownership (TCO).[5]

Calculating TCO depends on many variables, including acquisition, integration, deployment, support, and annual maintenance. Internal costs may add 30-50% to the total solution cost.[6] Organizations that choose to integrate multiple solutions for strong authentication will find that the costs proportionally multiply. As shown in the diagram below, both a premises-based solution operated by the business application provider and a solution hosted by a third-party service provider incur similar TCO.



The largest cost variable is supporting strong authentication for millions of consumers. For example, a physical USB token can cost $30 to $60. The distribution of the token requires packaging, postage and support. Physical tokens must be maintained and damaged or lost tokens replaced. Consumers may also need assistance configuring their smartphones with one or more credentials to enable SMS pings for automatic two-factor authentication (2FA) via cloud-based solutions. Helpdesks require additional staffing to support these requirements from external customers. One vendor's password support calculator cites analysts stating that between 20% and 50% of all helpdesk calls are for password resets; the average labor cost for one password reset is about $70.[7] It's difficult to predict the impact of supporting resets for traditional authentication factors on a mass scale.

Biometric factors are easier for consumers to use so they may help reduce overall TCO for a consumer solution. However, a tradeoff is higher initial cost per user: deploying a dedicated biometric solution is many times the cost of a sensor such as a fingerprint reader or retinal eye scanner. But the investment can pay big dividends. For example, following deployment of a Trusted Computing Module combined with biometrics for strong authentication, a bank with a nationwide staff of 8,000 reduced costs for password support by 98%.[8]

Other costs relate to potential risks and fallout of not deploying strong authentication. Some entities, including certain regulated industries, which do not comply with requirements to deploy strong authentication, may be subject to fines and penalties.

PASSWORD COMPLEXITY LEADS TO REUSE – AND A RESULTING BREACH AT ANOTHER SITE CAN ALSO LEAD TO A BREACH OF YOUR SITE.

Other costs incurred from data breaches include negative publicity, the loss of customers, loss of market share, and loss of market capitalization – all contributing to adverse fiscal impact.[9]

BARRIER 2: EASE OF USE

The ease of use barrier is why most consumer applications use a simple password for authentication. The business logic for this choice is that ease of use is a higher priority than security, and if the authentication process is too difficult consumers won't use the provider's application in the first place. Unfortunately, delegating security architecture decisions to consumers results in a very low quality of assurance.[10]

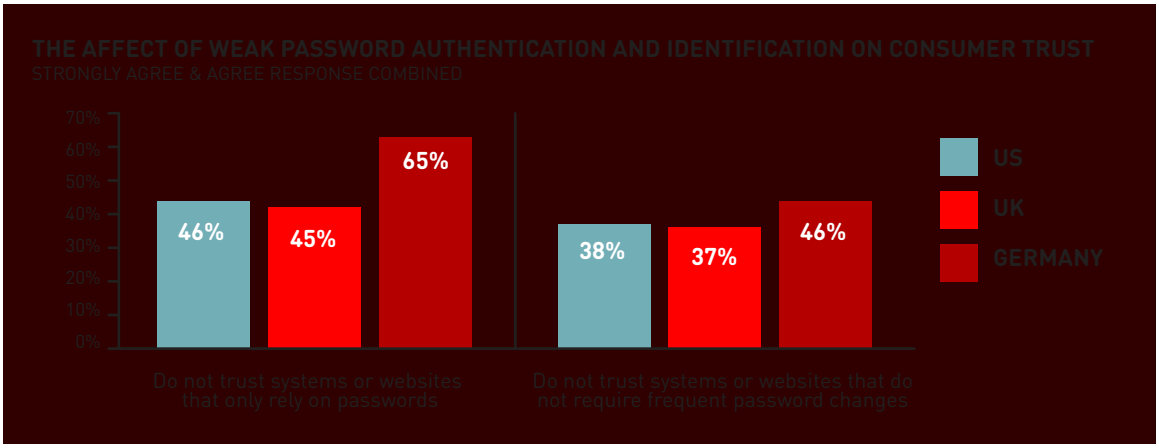
Some providers follow a strategy of giving consumers authentication that is simple enough to use without making them abandon the application, while injecting enough security to satisfy a minimal level of assurance. Unfortunately, this approach does not address the fact that the authentication barrier for consumer applications is not just about keeping the bad guys out. If it prevents legitimate customers from logging on, complaints will mount and the system will fail to deliver value to the end user.[11]

Part of the reluctance to "inflict" strong authentication on consumers may also be rooted in the past attitudes towards security education. A recent survey by Ponemon Institute shows a majority of consumers are wise to security risks. Consumers do not trust systems or websites that only rely on passwords or do not require frequent password changes. The perception of respondents as to the top five organizations that do the best online validation is (in order of best to worst): banking institutions, credit card and Internet payment providers, social media, retailers, and Internet service providers. [12]

When consumers feel uncomfortable with online security, they withdraw. For example, the abandonment of mobile shopping carts is very high. Of the 66% of smartphone and tablet users who have tried but failed to complete a transaction, 51% were uncomfortable entering credit card information.[13] Offering consumers strong authentication is validation of an application provider's concern for securing personal information--- it's the way to earn consumers' trust.

Toward this end, a wave of leading consumer applications is now offering two-factor authentication (also called "two-step") to help assuage consumers that their data is safe. During the last year or so, these include Google, Facebook, Dropbox, Apple, WordPress, Microsoft and Twitter. These schemes do require extra effort by users, and it is unclear how many of these services' users have enrolled in their two-step offerings.

For consumer applications that need strong authentication, there are increasing possibilities to maximize ease of use with the adoption of biometrics. Biometrics hold great promise as consumers are already familiar with access that is activated by a voice command, looking into an eye scanner, or pressing a fingertip or palm to a scanner. On a practical level, sensors for capturing biometrics are rapidly becoming prevalent for consumers in new-model smartphones. Since consumers rarely go anywhere without their smartphones, these devices offer huge potential for providing strong authentication into consumer applications. Eventually, the use of biometric factors will be a natural step that raises the level of security assurance for all end users.



BARRIER 3: SECURITY

Strengthening access security is a key function of strong authentication. The choice of using strong authentication depends on the level of assurance required for a particular use case. Example use cases are defined in the table below, drawn from specifications by the U.S. Office of Management and Budget and NIST. Applications requiring a high confidence in user identity must use strong authentication. Applications requiring moderate-to-low confidence in user identity may deploy a single-factor solution. While the level of trust is lower with a single factor, typically these applications do not require the expense, security and complexity of using multiple factors for authentication. When complexity increases, the tradeoff in usability must be considered. Traditional strong authentication becomes more complex to use with two- and especially three-factors.

LEVEL *	DESCRIPTION *	TOKEN (SECRET) **
1	Little or no confidence exists in the asserted identity; usually self-asserted; essentially a persistent identifier.	Allows any type of token including a simple PIN.
2	Confidence exists that the asserted identity is accurate; used frequently for self service applications.	Allows a single-factor authentication. Passwords are the norm at this level.
3	High confidence in the asserted identity's accuracy; used to access restricted data.	Multifactor authentication, typically a password or biometric factor used in combination with a 1) software token, 2) hardware token, or 3) OTP device token.
4	Very high confidence in the asserted identity's accuracy; used to access highly restricted data.	Multifactor authentication with a hardware crypto token.

* Office of Management and Budget 04-04
** NIST 800-63 Electronic Authentication Guideline

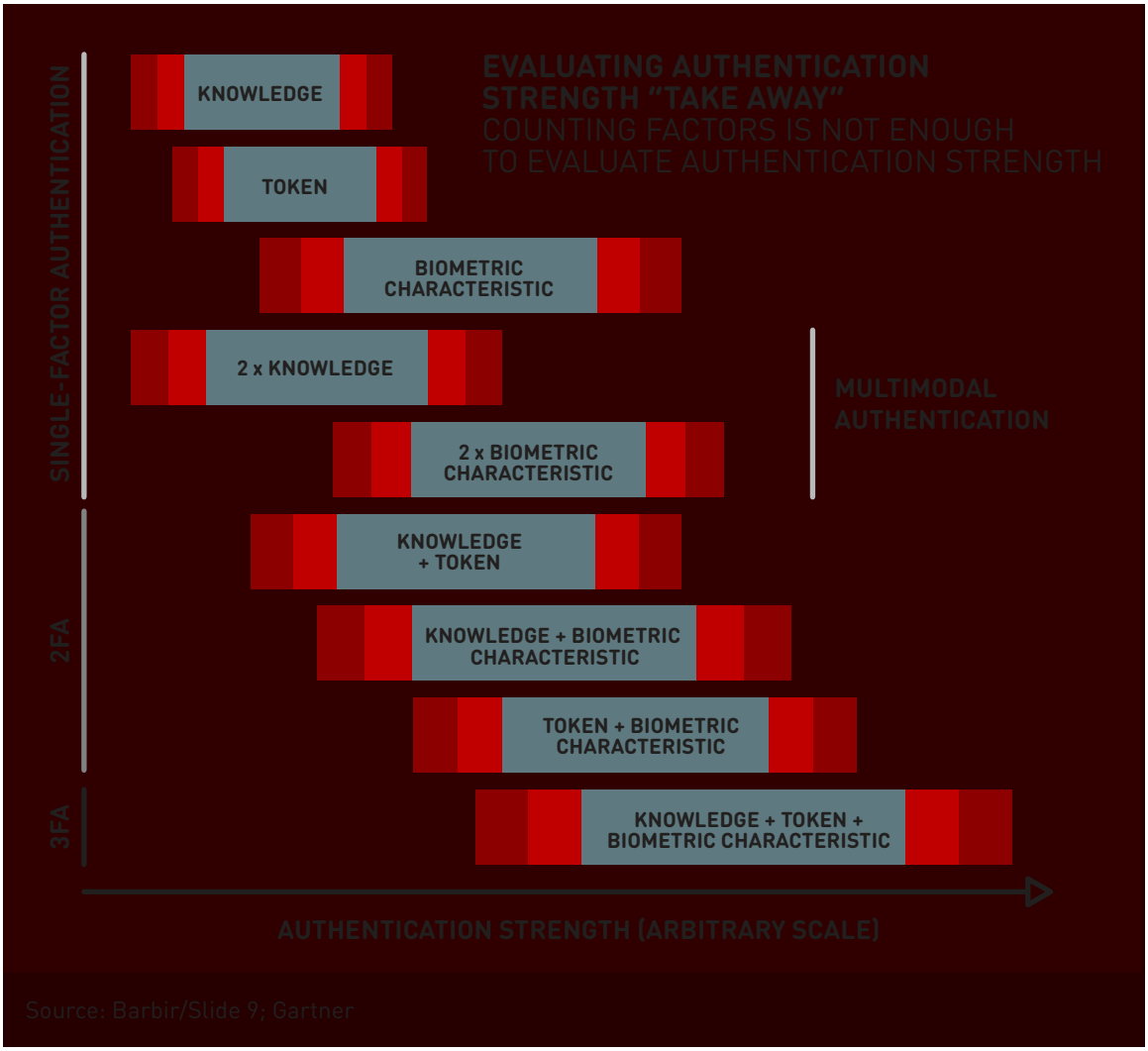
By definition, strong authentication uses more than one factor – but that does not automatically make it more secure. As noted in ISACA Journal (of the organization that manages the COBIT 5 framework for information security):[14]

- Two or more security factors can be combined to yield a strong multilayered solution, but only if they are all sound. Indeed, combining a weak factor with a stronger factor does not add much to the security provided.
- The selected factors, as used in the envisaged solution, must be mutually independent so that the compromising of one does not impact the protection level offered by the other(s).

The characteristics related to quality of an authentication factor include: 1) The factor is not forgettable; 2) the authentication codes generated are not guessable; 3) the factor is unfeasible to replicate; 4) the factor is not prone to be surreptitiously stolen via the Internet; and 5) the factor is tamper-resistant.

To overcome the barrier of security, factors used in an authentication solution should match the security strength requirements for the applicable consumer application. For example, if a consumer initiates a transaction with a smart phone and the SMS is sent to the same device, the SMS does not add any security to authentication. For this reason, Australian telecommunications companies have declared the use of SMS should no longer be considered a safe solution to verify identity during a banking transaction.[15]

The application of the above-mentioned characteristics in a strong authentication solution will result in a sliding scale of strength as shown in the figure below.[16]



BARRIER 4: PRIVACY

The privacy barrier relates to the ability of a strong authentication solution to secure factors stored in a user's authentication profile. The user's profile may include personally identifiable data such as name, address, birth date, birthplace, mother's maiden name, Social Security number (SSN), credit card information, or biometric information.All of these are stored somewhere in digital format and are at risk of a breach just like any other data. If centrally stored authentication data is breached, it can be duplicated, modified and used to the great detriment of the consumer application provider and its users.[17]

Biometric data is especially critical because if compromised in a server breach, the data can potentially be extracted. There are two classes of biometrics pertinent to authentication: anatomical/physiological factors and behavioral factors. Anatomical/physiological factors include fingerprints, palm prints, hand geometry, blood vessel patterns in the hand, patterns in the face, and patterns in the retina, to name a few. Behavioral factors include signature patterns and dynamics (while writing a signature), voice verification, and keystroke dynamics (such as the duration of each key press or time between keystrokes).[18]

Providers that centrally store biometric templates must ensure the safety of this sensitive data. Strong encryption can serve a protective role. For example, strong encryption is required by the Payment Card Industry Data Security Standard for all authentication credentials during transmission and storage on all payment card system components.[19] Another approach is using a digest or abstraction of biometric data to prevent exposure of the underlying biometric data.[20] A simpler approach is to remove the centralized storage risk and instead perform authentication with the biometric data stored on the end-user device.

Consumers may also appreciate strong authentication that preserves anonymity while using Internet resources. Privacy would be compromised if the authentication tool enabled activity tracking. Likewise, cloud solutions for strong authentication also must include safeguards to preserve privacy. To help stakeholders assess the privacy barrier, a candidate solution should undergo careful scrutiny using a comprehensive evaluation framework. One recent example is the MFA Cohortium's "Multi-Factor Authentication Solution Evaluation Criteria," which provides seven topics and 45 considerations for evaluation.[21]

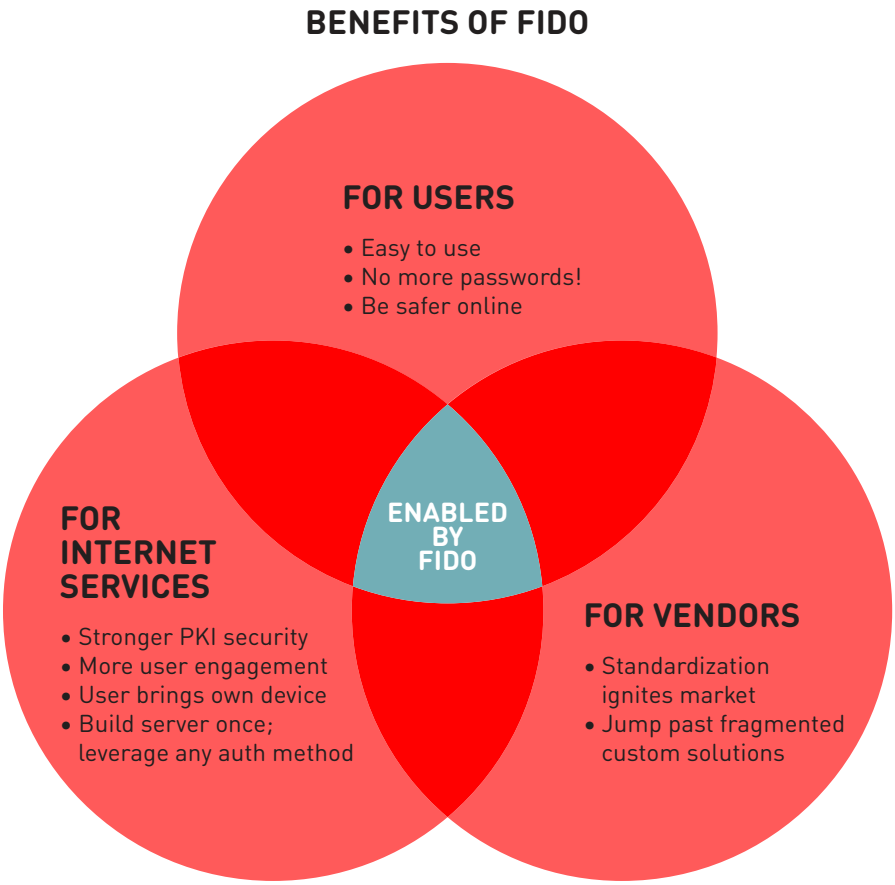
THE FIDO APPROACH REMOVES THE FOUR BARRIERS

The FIDO Alliance has created technical protocols that remove the four barriers to using strong authentication. The FIDO standards can be utilized by Internet service providers, component & device makers, and providers of software & stacks. By using FIDO, these stakeholders can lower costs, ensure consumer privacy, enforce stronger assurance of identity, and make strong authentication solutions easier to use.

Security professionals often believe that authentication is a continuum – easy to use if insecure at one end, and difficult to use but secure at the other. Pick the level of security and then dial up the corresponding level of pain that is inflicted on end users. But this perception is no longer true with FIDO. With FIDO, there doesn't have to be any tradeoff between ease-of-use and security! The FIDO protocols ensure that users receive strong security and the authentication experience is easy to use.

A key enabler for this is the latest generation of smartphones and tablets. Consumers carry these everywhere and are tuned into the need to protect personal information by locking their phones. PIN & Gesture are typical modes to unlock smartphones, and many are now enabled with finger scan, voice, facial recognition and other techniques to verify the user. These new biometric factors can be securely stored on the smartphones, and the FIDO protocols can be leverage by a strong authentication solution. No centrally stored authentication profiles are required.

Thanks to FIDO framework, everyone benefits!



LEARN HOW NOK NOK LABS CAN BRING FIDO SOLUTIONS TO YOU

We invite you to learn more about how Nok Nok Labs can help Internet services to provide consumers with simpler, stronger authentication. Your business can join the trend of consumer devices that provide simpler, stronger local authentication innovations. Why not leverage these today and remove all the barriers to using strong authentication?

ABOUT NOK NOK LABS

Nok Nok Labs, Inc., based in Palo Alto, CA, was founded to transform online authentication for modern computing. The company is backed by a team of security industry veterans from PGP, Netscape, Oracle, PayPal and Phoenix that have deep experience in building Internet scale security protocols and products. The company's ambition is to enable end-to-end trust across the web using authentication methods that are natural to end-users and provide strong proof of identity. For more information, visit www.noknok.com.

NOTES

1. One study says about 58% of online adults have five or more unique passwords, and more than 30% have 10 or more passwords; 2012 Online Registration & Password study by Janrain and Harris at http://janrain.com/about/newsroom/press-releases/online-americans-fatigued-by-password-overload-janrain-study-finds/; another says the average Internet user has 25 web accounts and performs eight daily logons using an average of 6.5 passwords at https://research.microsoft.com/pubs/74164/www2007.pdf.
2. Researchers found 56% of people mistype a password one in 10 times or more; see Jakobsson, M.; Shi, E.; Golle, P.; Chow, R. "Implicit authentication for mobile devices," 4th USENIX Workshop on Hot Topics in Security (HotSec '09); 11 August 2009; Montreal, Canada at http://www.parc.com/publication/2307/implicit-authentication-for-mobile-devices.html; summary here.
3. The top five passwords used during 2013 were: (1) 123456, (2) password, (3) 12345678, (4) qwerty, and (5) abc123; see http://www.cbsnews.com/news/the-25-most-common-passwords-of-2013/.
4. The National Institute of Standards and Technology (NIST) asked RAND to investigate why organizations choose to adopt or not adopt strong authentication, and where they choose to use it. The biggest influences were compulsion by law or regulation, or customer expectations. Other factors had minimal effect. See M. Libicki, E. Balkovich, B. Jackson, R. Rudavsky, and K. Watkins Webb, "Influences on the Adoption of Multifactor Authentication," RAND Homeland Security and Defense Center (2011) at http://www.rand.org/pubs/technical_reports/TR937.html.
5. Symantec Corporation, "Two-Factor Authentication: A TCO Viewpoint" (2012).
6. PhoneFactor, "Guide to Evaluating Multifactor Authentication Solutions"; PhoneFactor became Microsoft Windows Azure Multi-Factor Authentication in 2012.
7. Mandylion Research Labs, Password Cost Estimator at http://www.mandylionlabs.com/PRCCalc/PRCCalc.htm.
8. Trusted Computing Group, "Multi-Factor Authentication – The Real Truth in the Real World" (2011).
9. The average global cost-per-record breached is $136 ($188 in the U.S.); see Ponemon Institute, "2013 Cost of a Data Breach Study: Global Analysis," (April 2013). A financial analyst projected the total cost of Target's late 2013 breach at over $1 billion; see http://www.bizjournals.com/twincities/news/2014/01/31/targets-breach-costs-billion-dollars.html?page=all.
10. See again the list of most popular passwords used during 2013 at http://www.cbsnews.com/news/the-25-most-common-passwords- of-2013/.
11. Bruce Schneier, "Balancing Security and Usability in Authentication," 19 February 2009.
12. Ponemon Institute, Forget Passwords: How Consumers Want Their Identity Authenticated A Study of US, UK and German Consumers (April 2013).
13. Jumio 2013 Consumer Mobile Insights Study.
14. Alessandro Campi, "How Strong is Strong User Authentication?" ISACA Journal (2012) Vol. 5.
15. "Telcos Declare SMS 'Unsafe' for Bank Transactions," IT News for Australian Business (9 Nov. 2012) at http://www.itnews.com.au/News/322194,telcos-declare-sms-unsafe-for-bank-transactions.aspx.
16. Abbie Barbir, Co-chair OASIS Trust Elevation TC, "Multi-factor Authentication Methods Taxonomy," (7 March 2013).
17. A good example are the breaches at Experian & Bothers, which led a Garter analyst to declare that knowledge-based authentication is dead; see Avivah Litan, "The Death of KBA; Secret life questions fluster Obamacare applicants (23 Oct. 2013) at http://blogs.gartner.com/avivah-litan/2013/10/23/the-death-of-kba-secret-life-questions-fluster-obamacare-applicants/. Also see Krebs on Security, "Data Broker Giants Hacked by ID Theft Service" (25 Sept. 2013) at http://krebsonsecurity.com/2013/09/data-broker-giants-hacked-by-id-theft-service/.
18. Anna Schlenker and Milan Sarek, "Behavioural Biometrics for Multi-Factor Authentication in Biomedicine," EJBI, Vol. 8 (2012), Issue 5, pp. 19-24.
19. PCI DSS 8.2.1.
20. Kikelomo Maria Apampa, Tian Zhang, Gary B Wills, and David Argles, "Ensuring Privacy of Biometric Factors in Multi-Factor Authentication Systems," SECRYPT 2008, International Conference on Security and Cryptography in ICETE 08, Porto, Portugal, 26 - 29 Jul 2008.
21. The MFA Cohortium, "Multi-Factor Authentication Solution Evaluation Criteria" (2013).

ABOUT NOK NOK LABS

Backed by a management team of security industry veterans from PGP, Netscape, PayPal and Phoenix, Nok Nok Labs have a deep experience in building Internet scale security protocols and products. Our ambition is to fundamentally transform authentication, by unifying authentication into one standard protocol, giving business the power to make the utmost of the cloud, data, mobile and business online.

Nok Nok Labs
4151 Middlefield Road, Suite 200
Palo Alto, CA 94303 USA

www.noknok.com

TO LEARN MORE ABOUT NOK NOK LABS,
VISIT NOKNOK.COM OR CONTACT US
AT INFO@NOKNOK.COM

Nok Nok
LABS