

TRENDS IN U.S. MULTI-FACTOR NON-COMPLIANCE

an evaluation of how US financial institutions are avoiding compliance with
FFIEC multi-factor authentication guidelines, and the implications for online consumer privacy

© 2007 Sestus Data Company. Personal use of this material is permitted, however, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the author. Points of view in this document are those of the authors and do not necessarily represent the official position of the FFIEC or the FDIC. Published June 21, 2007.

Abstract

We evaluate website authentication methods against a statistical sampling of 100 U.S. banks with published website statements asserting their belief in their compliance with FFIEC multi-factor authentication (MFA) guidelines.

The purpose of the evaluation is to 1) identify the authentication methods used by each bank, 2) determine compliance with published FFIEC multi-factor authentication guidelines, 3) report on apparent mis-interpretations of the FFIEC's definition of multi-factor authentication, and 4) postulate the effects of implemented authentication methods to online privacy.

Findings

We find 1) overwhelming use of single-factor challenge/response, image-based, and other knowledge-based authentication methods purporting to be multi-factor authentication, 2) numerous and varied mis-interpretations regarding the definition of "something the user has", and 3) a high probability for increasing online fraud and loss of consumer privacy as a result of widespread adoption of challenge/response and other knowledge-based systems.

1 DEFINITION OF MULTI-FACTOR AUTHENTICATION

On October 12, 2005, the Federal Financial Institutions Examination Council (FFIEC) issued an updated guidance letter for banks and financial institutions which made the following recommendation:

"The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. Single-factor authentication tools, including passwords and PINs, have been widely used for a variety of Internet banking and

electronic commerce activities, including account inquiry, bill payment, and account aggregation. However, financial institutions should assess the adequacy of such authentication techniques in light of new or changing risks such as phishing, pharming, malware, and the evolving sophistication of compromise techniques. Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks." (FFIEC, "Authentication in an Internet Banking Environment" October 12, 2005 Page 4)

In this same document, the FFIEC defined the three authentication "factors" thus:

"Existing authentication methodologies involve three basic "factors":

- Something the user *knows* (e.g., password, PIN);
- Something the user *has* (e.g., ATM card, smart card); and
- Something the user *is* (e.g., biometric characteristic, such as a fingerprint)." (FFIEC, "Authentication in an Internet Banking Environment" October 12, 2005 Page 3)

On August 15, 2006, the Federal Financial Institutions Examination Council (FFIEC) issued a Supplement in which it clarified what it considered to be "true multi-factor authentication":

"By definition true multifactor authentication requires the use of solutions from two or more of the three categories of factors. Using multiple solutions from the same category at different points in the process may be part of a layered security or other compensating control approach, but it would not constitute multifactor authentication." (FFIEC, "Frequently Asked Questions on FFIEC Guidance on Authentication in an Internet Banking Environment" August 15, 2005 Page 6)

2 REPRESENTATIVE SAMPLE

We conducted a search using Windows® Live Search® for U.S. financial institutions with websites asserting multi-factor compliance. From the search results returned we selected a representative sample based on the following criteria: 1) the organization is a U.S. bank regulated by the FFIEC, 2) the organization asserts on its website its belief that it is in compliance with FFIEC multi-factor authentication guidelines, and 3) the organization describes its authentication methodology on its website. Using these criteria, 100 banks were selected at random irrespective of size, location, or member demographics. No other filtering or screening was applied.

3 EVALUATION PROCESS

We evaluated each bank's login process for "true multi-factor authentication" as defined by the FFIEC in their August 2006 Supplement cited above. In keeping with the FFIEC published definition of multi-factor authentication, we classified each authentication element as either "something the user knows", "something the user has", or "something the user is".

Login IDs, passwords, PINs, personal information solicited in response to challenge questions, visual images, captchas displaying random codes, textual phrases are all examples of things that users "know". Regardless of how the information may be solicited, displayed, or entered, if the information is not obtained from a tangible physical object in the possession of the user, it is, by definition, "something the user knows".

Objects in the user's physical possession such as hardware tokens, smartcards, out-of-band email or telephone information, and information retrieved from a user's computer such as cookie file information or digital certificates are all examples of things that users "have". Anything that is retrieved from a tangible, physical object in the possession of the user, including information retrieved from out-of-band email or telephone, is "something the user has".

While biometric authentication methods such as iris scans, thumbprints, and voice prints are legitimate examples of "something the user is", none of the banks in the sample evidenced any biometric authentication factors.

Banks that did not consistently employ "solutions from two or more of the three categories of factors" were rated as non-compliant with FFIEC multi-factor authentication guidelines.

A note on *consistency*: The FFIEC does not recommend multi-factor authentication "sometimes" or "only when convenient". It recommends multi-factor authentication whenever the user desires "access to customer information or the movement of funds to other parties".

Some banks do not consistently employ "solutions from two or more of the three categories of factors", switching from multi-factor to single-factor when necessary. These banks may initially attempt to detect "something the user has" and then revert to soliciting more of "something the user knows" when they are unable to detect the desired "something the user has" authentication factor.

For example, a bank may attempt to retrieve cookie file information or a software certificate from the user's computer. If this information can be obtained in every case, we consider the bank to be compliant with the FFIEC's multi-factor authentication guidelines. However, if this information cannot be obtained in every case, such as when a cookie file has been erased by the user, since the bank does not detect "something the user has" we consider the bank to not be compliant.

4 FINDINGS

4.1 Single-Factor Authentication Persists

Despite published assertions of multi-factor compliance, we find overwhelming use of single-factor challenge /response, image-based, and other knowledge-based authentication methods purporting to be FFIEC-compliant multi-factor authentication.

Within the sample group:

Consistently Multi-Factor

Only **4%** of the sampled banks employed consistently multi-factor authentication methods.

Inconsistently Multi-Factor

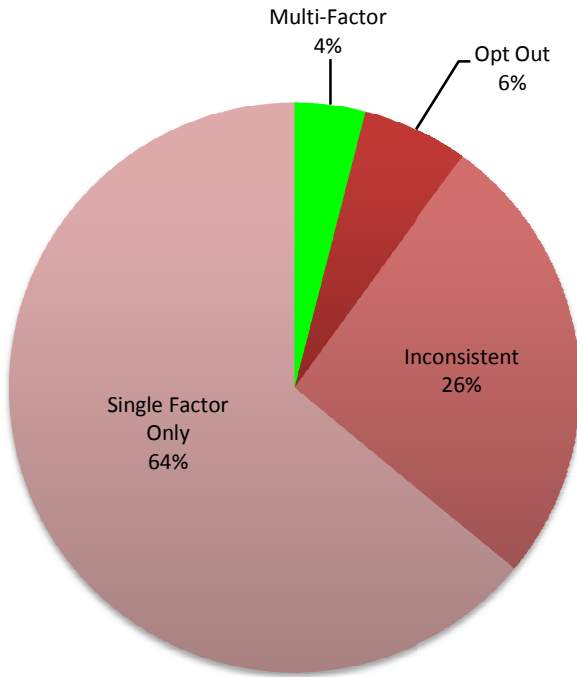
26% of the sampled banks employed authentication methods that were inconsistently multi-factor. They occasionally detected "something the user has" but reverted to entirely single-factor authentication methods, soliciting more of "something the user knows" when they were unable to detect the "something the user has" authentication factor.

Permits "opt out" of Multi-Factor

6% of the sampled banks offered consistently multi-factor out-of-band approaches as an *option* but permitted users to choose other single-factor authentication options instead.

Single-Factor Only

64% of the sampled banks were entirely single-factor, relying only on solicited personal information and/or shared secret images. Nothing was retrieved for the “something the user has” authentication factor.



4.2 Mis-Representation and Confusion Regarding “Something the User Has”.

We find ad-hoc interpretation, mis-representations, and generally incorrect statements regarding the definition of what constitutes “something the user has”, a key element of “true multi-factor authentication”.

Within the sample group:

Proper Definition

4% of the sampled banks properly described “something the user has” as involving tangible objects in the user’s physical possession such as hardware tokens, smartcards, out-of-band email or telephone information, and information retrieved from a user’s computer such as cookie file information, or digital certificates.

Challenge Questions Mis-represented as “Something the user has”

96% of the sampled banks mis-represented or implied that personal information solicited via challenge questions would meet the regulatory definition of “something the user has” instead of the correct “something the user knows”.

Curiously, while the sampled banks generally quoted the regulatory definition correctly, most then proceeded to mis-represent personal information solicited via challenge questions as “something the user has” instead of the correct “something the user knows”.

The sampled banks also mis-represented numerous other knowledge-based elements as “something the user has”, including captchas, shared-secret images, and credentials entered through on-screen sliders, dials, and keypads, all of which are simply methods for soliciting, displaying, verifying, or entering “known” information.

We saw considerable mis-representation of shared-secret images as “something the user has” instead of the correct “something the user knows”. An image is a visual representation of “shared secret” information, i.e. “something the user knows” that is shared between the user and the bank. The bank is expecting the user to “know” whether or not the image they display on-screen is correct. Since the image is not a tangible physical object whose possession by the user can be detected by the bank, but is simply visual information displayed on the screen for recognition purposes, it is “something the user knows”, not “something the user has”.

4.3 Loss of Consumer Privacy Likely to Increase.

The FFIEC recommended implementing multi-factor authentication in an attempt to protect consumer privacy in the face of exploding phishing, pharming, and online fraud.

U.S. financial institutions, however, appear to be rejecting those guidelines in favor of knowledge-based approaches that solicit even more personal information from consumers in the form of challenge questions.

We found widespread implementation of single-factor challenge/response and shared-secret image-based approaches purporting to be FFIEC-compliant multi-factor authentication. Such universal solicitation of previously undisclosed personal information to facilitate authentication does not bode well for consumer privacy.

A Change for the Worse

With the widespread implementation of challenge/response systems, consumers should expect fraudsters to increase their efforts to discover confidential personal information where they had previously focused their efforts on discovering relatively anonymous logins and passwords.

These types of attacks have already been launched against early adopters of challenge/response systems. The Washington Post reported last year on a "new" type of phishing attack against Bank of America's Sitekey system in which the fraudster asked victims on a fictitious bank website to enter their previously registered personal information "for verification purposes", precisely the same process and reason given by the legitimate bank for requesting the same information.

The widespread adoption of challenge/response systems will encourage similar solicitation and theft of confidential personal information. The stage is being set for an online privacy crisis fueled by millions of pieces of previously-undisclosed personal information solicited by thousands of legitimate financial websites as well as by tens of thousands of fraudulent websites.

The U.S. Federal Deposit Insurance Corporation (the FDIC) has already issued cautionary statements against the use of solicited personal information for authentication purposes. On Jun 17, 2005, the FDIC published a supplement to an earlier report in which it repeatedly cautioned financial organizations regarding using personal information in the authentication process:

"Although consumers are worried about phishing and the trustworthiness of e-mail messages from their banks, they are also concerned about the security of their personal information more generally."

"When banks consider authentication methods for retail customers, they should be aware that these customers value security and the protection of confidential information... Consumers will require a clear explanation of any security mechanism and the use of any personal information required to implement that security mechanism."

"Limitations on the use of personal information and the existence of privacy safeguards are important elements of consumer acceptance."

"Consumers are also concerned about the risk associated with large databases of personal information and the potential for the information that is used by authentication methods to be compromised, copied, or imitated." (FDIC, "Putting an End to Account-Hijacking Identity Theft: Study Supplement" June 17, 2005)

The FFIEC's multi-factor authentication guidelines went into effect approximately six months ago. To date, the FFIEC has shown considerable leniency in holding banks and other financial institutions accountable for complying with its multi-factor guidelines. However, with such a large percentage of banks mis-representing or ignoring those published guidelines, the FFIEC is now faced with an unpleasant choice. They must decide whether to hold banks more closely accountable for adhering to their published multi-factor guidelines, or loosen their standards and permit the widespread solicitation of previously undisclosed confidential consumer information.

Enforcement of FFIEC's existing multi-factor guidelines may be advisable at this time, perhaps simultaneous with the publication of a statement similar to that issued by the FDIC in 2005 cautioning against the solicitation of personal information for authentication purposes.

5 SAMPLED DATA

Legend:

Y	=	Yes (Authentication factor present = Compliant)
N	=	No (Authentication factor not present = Non-Compliant)
TOK	=	Hardware Tokens (Compliant)
OOB	=	Out-of-Band Multi-Factor (Compliant)
INC	=	Inconsistently Multi-Factor (Multi-factor Sometimes/Single-Factor sometimes =Non-Compliant)
OPT	=	Permits user to "Opt Out" of Multi-Factor (Non-Compliant)

Bank #	"Know"	"Has"	"Is"	Notes
1	Y	N	N	No "something the user has" element found. Uses only challenge/response
2	Y	TOK	N	Hardware tokens for all members
3	Y	N	N	No "something the user has" element found. Uses only challenge/response
4	Y	INC	N	If cookie file not found, reverts to solicitation of personal information
5	Y	N	N	No "something the user has" element found. Uses only challenge/response
6	Y	N	N	No "something the user has" element found. Uses only challenge/response
7	Y	N	N	No "something the user has" element found. Uses only challenge/response
8	Y	OPT	N	Out-of-band only option available, as well as challenge/response option
9	Y	N	N	No "something the user has" element found. Uses only challenge/response
10	Y	N	N	No "something the user has" element found. Uses only challenge/response
11	Y	N	N	No "something the user has" element found. Uses only challenge/response
12	Y	N	N	No "something the user has" element found. Uses only challenge/response
13	Y	INC	N	If cookie file not found, reverts to solicitation of personal information
14	Y	N	N	No "something the user has" element found. Uses only challenge/response
15	Y	OOB	N	Out-of-band used when cookie file not found
16	Y	INC	N	If cookie file not found, reverts to solicitation of personal information
17	Y	OPT	N	Out-of-band only option available, as well as challenge/response option
18	Y	N	N	No "something the user has" element found. Uses only challenge/response
19	Y	N	N	No "something the user has" element found. Uses only challenge/response
20	Y	INC	N	If cookie file not found, reverts to solicitation of personal information
21	Y	OPT	N	Out-of-band only option available, as well as challenge/response option
22	Y	N	N	No "something the user has" element found. Uses only challenge/response
23	Y	N	N	No "something the user has" element found. Uses only challenge/response
24	Y	INC	N	If cookie file not found, reverts to solicitation of personal information
25	Y	INC	N	If cookie file not found, reverts to solicitation of personal information
26	Y	N	N	No "something the user has" element found. Uses only challenge/response
27	Y	INC	N	If cookie file not found, reverts to solicitation of personal information
28	Y	N	N	No "something the user has" element found. Uses only challenge/response
29	Y	INC	N	If cookie file not found, reverts to solicitation of personal information
30	Y	N	N	No "something the user has" element found. Uses only challenge/response
31	Y	N	N	No "something the user has" element found. Uses only challenge/response
32	Y	N	N	No "something the user has" element found. Uses only challenge/response
33	Y	N	N	No "something the user has" element found. Uses only challenge/response
34	Y	N	N	No "something the user has" element found. Uses only challenge/response

Bank #	"Know"	"Has"	"Is"	Notes
35	Y	N	N	No "something the user has" element found. Uses only challenge/response
36	Y	N	N	No "something the user has" element found. Uses only challenge/response
37	Y	INC	N	If cookie file not found, reverts to solicitation of personal information
38	Y	N	N	No "something the user has" element found. Uses only challenge/response
39	Y	N	N	No "something the user has" element found. Uses only challenge/response
40	Y	N	N	No "something the user has" element found. Uses only challenge/response
41	Y	N	N	No "something the user has" element found. Uses only challenge/response
42	Y	INC	N	If cookie file not found, reverts to solicitation of personal information
43	Y	OPT	N	Out-of-band only option available, as well as challenge/response option
44	Y	INC	N	If cookie file not found, reverts to solicitation of personal information
45	Y	INC	N	If cookie file not found, reverts to solicitation of personal information
46	Y	INC	N	If cookie file not found, reverts to solicitation of personal information
47	Y	N	N	No "something the user has" element found. Uses only challenge/response
48	Y	N	N	No "something the user has" element found. Uses only challenge/response
49	Y	N	N	No "something the user has" element found. Uses only challenge/response
50	Y	N	N	No "something the user has" element found. Uses only challenge/response
51	Y	N	N	No "something the user has" element found. Uses only challenge/response
52	Y	INC	N	If cookie file not found, reverts to solicitation of personal information
53	Y	INC	N	If cookie file not found, reverts to solicitation of personal information
54	Y	N	N	No "something the user has" element found. Uses only challenge/response
55	Y	N	N	No "something the user has" element found. Uses only challenge/response
56	Y	OOB	N	Out-of-band used when cookie file not found
57	Y	N	N	No "something the user has" element found. Uses only challenge/response
58	Y	N	N	No "something the user has" element found. Uses only challenge/response
59	Y	N	N	No "something the user has" element found. Uses only challenge/response
60	Y	N	N	No "something the user has" element found. Uses only challenge/response
61	Y	INC	N	If cookie file not found, reverts to solicitation of personal information
62	Y	N	N	No "something the user has" element found. Uses only challenge/response
63	Y	INC	N	If cookie file not found, reverts to solicitation of personal information
64	Y	N	N	No "something the user has" element found. Uses only challenge/response
65	Y	N	N	No "something the user has" element found. Uses only challenge/response
66	Y	N	N	No "something the user has" element found. Uses only challenge/response
67	Y	N	N	No "something the user has" element found. Uses only challenge/response
68	Y	N	N	No "something the user has" element found. Uses only challenge/response
69	Y	N	N	No "something the user has" element found. Uses only challenge/response
70	Y	N	N	No "something the user has" element found. Uses only challenge/response
71	Y	N	N	No "something the user has" element found. Uses only challenge/response
72	Y	N	N	No "something the user has" element found. Uses only challenge/response
73	Y	INC	N	If cookie file not found, reverts to solicitation of personal information
74	Y	N	N	No "something the user has" element found. Uses only challenge/response
75	Y	INC	N	If cookie file not found, reverts to solicitation of personal information
76	Y	INC	N	If cookie file not found, reverts to solicitation of personal information
77	Y	INC	N	If cookie file not found, reverts to solicitation of personal information
78	Y	TOK	N	Hardware tokens for all members
79	Y	N	N	No "something the user has" element found. Uses only challenge/response
80	Y	INC	N	If cookie file not found, reverts to solicitation of personal information

TRENDS IN U.S. MULTI-FACTOR NON-COMPLIANCE

an evaluation of how US financial institutions are avoiding compliance with FFIEC multi-factor authentication guidelines, and the implications for online consumer privacy
 © 2007 Sestus Data Company. Published June 21, 2007.

Bank #	"Know"	"Has"	"Is"	Notes
81	Y	INC	N	If cookie file not found, reverts to solicitation of personal information
82	Y	N	N	No "something the user has" element found. Uses only challenge/response
83	Y	N	N	No "something the user has" element found. Uses only challenge/response
84	Y	INC	N	If cookie file not found, reverts to solicitation of personal information
85	Y	N	N	No "something the user has" element found. Uses only challenge/response
86	Y	N	N	No "something the user has" element found. Uses only challenge/response
87	Y	N	N	No "something the user has" element found. Uses only challenge/response
88	Y	N	N	No "something the user has" element found. Uses only challenge/response
89	Y	N	N	No "something the user has" element found. Uses only challenge/response
90	Y	N	N	No "something the user has" element found. Uses only challenge/response
91	Y	OPT	N	Out-of-band only option available, as well as challenge/response option
92	Y	N	N	No "something the user has" element found. Uses only challenge/response
93	Y	N	N	No "something the user has" element found. Uses only challenge/response
94	Y	N	N	No "something the user has" element found. Uses only challenge/response
95	Y	N	N	No "something the user has" element found. Uses only challenge/response
96	Y	N	N	No "something the user has" element found. Uses only challenge/response
97	Y	INC	N	If cookie file not found, reverts to solicitation of personal information
98	Y	INC	N	If cookie file not found, reverts to solicitation of personal information
99	Y	N	N	No "something the user has" element found. Uses only challenge/response
100	Y	OPT	N	Out-of-band only option available, as well as challenge/response option

Study Co-Authors:



Sestus Data Company's PhishCops™ product is based on government-approved authentication methods and the U.S. government has recognized PhishCops™ for its breakthrough in multi-factor authentication, naming it a semi-finalist for both the 2005 and 2007 Homeland Security Award. PhishCops™ is also a recipient of the InfoWorld 100 Award, InfoWorld Magazine's highest honor for technical innovation.

PhishCops™ enjoys an enviable reputation in the financial market with organizations and consumers. The company credits its positive reception to its patent-pending approach to authentication which never solicits personal information.

Media Contact:
 Tel: (800) 788-1927 ext 1
 Fax (800) 741-9048
 Email: info@sestusdata.com

Websites:
<http://www.sestusdata.com>
<http://www.phishcops.com>



The BearingPoint Financial Services Information Security group provides information security services to large and midsized financial services companies. Led by Warren Zafrin, Karim Zerhouni and Peter Robinson, the group works with clients to protect their data, comply with federal and international laws and regulations, reduce operational and reputation risks, and imbed security into their next-generation financial services products and services.

BearingPoint is a leading management and technology consulting company serving the Forbes Global 2000 and many of the world's largest public services organizations. The company's 6,000 risk, compliance and security professionals are skilled in both strategy and execution. Operating in more than 40 countries, they are dedicated to providing tailored, effective strategy, process and technology solutions.

To learn more, call 1 866 BRNGPNT (+1 508 216 2523 from outside US and Canada) or visit www.bearingpoint.com.