The Banking Law Journal

Established 1889

An A.S. Pratt® PUBLICATION JULY/AUGUST 2017

EDITOR'S NOTE: THE SUMMER READING ISSUE
Victoria Prussen Spears

CONSTRUCTION LOAN GUARANTEES
Mitchell S. Kaplan

THE PASSWORD IS DEAD; IS KNOWLEDGE-BASED AUTHENTICATION FAR BEHIND?
Nicholas R. Merker, Nicole R. Woods, and Blaine L. Dirker

COURT GUTS LYONDELL TRUSTEE'S BANKRUPTCY-RELATED CLAIMS
Michael L. Cook

CHAPTER 22 COMMENCEMENT TO CONFIRMATION IN JUST SIX DAYS: EXPLORING *ROUST CORPORATION*
Andriana Georgallas

NOTICE OVER SCIENCE: DELAWARE BANKRUPTCY COURT ENFORCES BAR DATE AGAINST ASBESTOS CREDITOR BASED ON ACTUAL NOTICE STANDARD
Patrick M. Steel

UPHEAVAL IN THE GERMAN RESTRUCTURING MARKET: NEED-TO-KNOW FACTS, ALTERNATIVE TOOLS, AND NEW DRAFT LAW
Thomas Fox, Frank Grell, Hendrik Hauke, Tobias Klass, and Jörn Kowalewski

CREATION AND DEVELOPMENT OF THE BASEL COMMITTEE ON BANKING SUPERVISION AND THE RESULTING AGREEMENTS
Stanyo Neykov Dinov

LexisNexis

THE BANKING LAW JOURNAL

VOLUME 134 **NUMBER 7** **July/August 2017**

Editor's Note: The Summer Reading Issue
Victoria Prussen Spears 367

Construction Loan Guarantees
Mitchell S. Kaplan 369

The Password Is Dead; Is Knowledge-Based Authentication Far Behind?
Nicholas R. Merker, Nicole R. Woods, and Blaine L. Dirker 375

Court Guts Lyondell Trustee's Bankruptcy-Related Claims
Michael L. Cook 379

Chapter 22 Commencement to Confirmation in Just Six Days: Exploring *Roust Corporation*
Andriana Georgallas 387

Notice Over Science: Delaware Bankruptcy Court Enforces Bar Date Against Asbestos Creditor Based on Actual Notice Standard
Patrick M. Steel 390

Upheaval in the German Restructuring Market: Need-to-Know Facts, Alternative Tools, and New Draft Law
Thomas Fox, Frank Grell, Hendrik Hauke, Tobias Klass, and Jörn Kowalewski 393

Creation and Development of the Basel Committee on Banking Supervision and the Resulting Agreements
Stanyo Neykov Dinov 399

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please call:

Matthew T. Burke at ..... (800) 252-9257
Email: ..... matthew.t.burke@lexisnexis.com
Outside the United States and Canada, please call . . . . . (973) 820-2000

For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at . . . . . (800) 833-9844
Outside the United States and Canada, please call . . . . . (518) 487-3385
Fax Number . . . . . (800) 828-8341
Customer Service Website . . . . . http://www.lexisnexis.com/custserv/

For information on other Matthew Bender publications, please call

Your account manager or . . . . . (800) 223-1940
Outside the United States and Canada, please call . . . . . (937) 247-0293

ISBN: 978-0-7698-7878-2 (print)
ISBN: 978-0-7698-8020-4 (eBook)
ISSN: 0005-5506 (Print)
ISSN: 2381-3512 (Online)

Cite this publication as:

The Banking Law Journal (LexisNexis A.S. Pratt)

Because the section you are citing may be revised in a later release, you may wish to photocopy or print out the section for convenient future reference.

An A.S. Pratt® Publication

Editorial Office
230 Park Ave., 7th Floor, New York, NY 10169 (800) 543-6862
www.lexisnexis.com

MATTHEW BENDER

Editor-in-Chief, Editor & Board of Editors

THE BANKING LAW JOURNAL (ISBN 978-0-76987-878-2) (USPS 003-160) is published ten times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices.

For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer. Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 718.224.2258 (phone). Material for publication is welcomed— articles, decisions, or other items of interest to bankers, officers of financial institutions, and their attorneys.

the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to THE BANKING LAW JOURNAL LexisNexis Matthew Bender, 230 Park Ave, 7th Floor, New York, NY 10169.

POSTMASTER: Send address changes to THE BANKING LAW JOURNAL, A.S. Pratt & Sons, 805 Fifteenth Street, NW., Third Floor, Washington, DC 20005-2207.

The Password Is Dead; Is Knowledge-Based Authentication Far Behind?

Nicholas R. Merker, Nicole R. Woods, and Blaine L. Dirker[*]

Knowledge-based authentication ("KBA") can be a valuable tool against fraud, but to what degree ultimately falls on those corporations and financial institutions which rely on it as an authentication mechanism. The authors of this article discuss the problems with KBA, and offer some steps users can take now to strengthen security when using KBA.

Whether you know it or not, you are likely familiar with knowledge-based authentication ("KBA"). If you have ever provided an answer to a "secret" question to log on to a device or access an account, then you have used KBA.

WHAT EXACTLY IS KBA?

So what exactly is KBA? KBA is an identity authentication method used to test your knowledge about you, the owner of your identity. Since your answer should be known only by you, the user, one might presume that such information would be relatively secure. It turns out, however, that most of your information associated with KBA is far from it.

Passwords, while seemingly ubiquitous, may have found the end of their usefulness—more often than not, most passwords can be guessed, obtained by a key logger, or broken by brute force. In other words, no matter how unique or lengthy or complex a password is, it may not be enough to completely secure data. This has led many pundits to proclaim the password is dead, despite its continued use and reliance.

Enter KBA: the security question(s) and answer(s) that can be used in addition to your password. KBA is generally either static or dynamic. Static KBA allows you to select from a set of pre-determined questions, such as "What is the name of your first pet?" or "What was the name of your high school?" Dynamic KBA generates questions dynamically that would only apply to one specific person. Commonly referred to as "out-of-wallet" KBA, to signify that the information could not be determined from the information typically contained in a person's wallet, such questions are generated from your credit

---

[*] Nicholas R. Merker is a partner at Ice Miller LLP and co-chair of its Data Security and Privacy Practice. Nicole R. Woods is an associate at the firm focusing her practice on complex commercial litigation. Blaine L. Dirker is of counsel in the firm's Intellectual Property and Data Security and Privacy groups. The authors may be reached at nicholas.merker@icemiller.com, nicole.woods@icemiller.com, and blaine.dirker@icemiller.com, respectively.

history or public records. Such dynamic KBA questions might ask "What was the name of the school you attended when you were 10 years old?" or "What year did you purchase your Jeep Wrangler?" Regardless of whether the KBA questions are static or dynamic, the assumption is that only you know the correct answers to the "secret" questions, thereby confirming your identity.

WHAT'S SO WRONG WITH USING KBA?

In the infancy of the internet, KBA appeared useful as a secondary form of authentication for determining one's access to restricted accounts, resetting passwords, etc. It was presumed that only the user or those in the user's inner circle could know the type of information being requested by the security questions. Now, however, thanks to the predominant use of social media, the power of internet search engines, and access to public records via the internet, your personal information may only be a few keystrokes away.

One of the earliest public examples of the vulnerability of KBA came in 2008 from then-Alaska Governor Sarah Palin. A hacker was able to obtain access to Palin's personal Yahoo email account. The hacker purportedly posted an explanation of how he gained access to the account on an internet message board. The description detailed how easily question and answer KBA can be broken. The hacker requested to reset Palin's Yahoo email account password and was asked three questions: Palin's birthdate, her zip code, and the location of where she met her spouse. A quick internet search provided the answer to each one of these questions. From there, the hacker was able to reset the password and had exclusive access to Palin's personal emails.

More recently, the cybercriminals have gained access to taxpayer information "secured" by the Internal Revenue Service ("IRS") by answering KBA questions intended to prevent such access. In 2015, cybercriminals accessed the IRS's "Get Transcript" program using personally identifiable information (e.g., names, addresses, social security numbers, etc.) to answer KBA questions, which allowed the cybercriminals to download prior year's income tax returns and file phony tax returns to claim fraudulent refunds. Similarly, in 2016, cybercriminals breached the IRS's E-File PIN application by answering KBA questions required to retrieve forgotten PINs. As a result, more than 100,000 social security numbers were compromised.

In the day and age of booming social media, an alarming amount of so-called "secret" personal information is available for anyone to see. In 2016, 78 percent of Americans had some type of social media profile. As of February 1, 2017, there are over 1.86 billion monthly active Facebook users with 293,000 statuses

updated and 136,000 photos uploaded every 60 seconds. That vast amount of sometimes highly-personal information is now a source of potential fodder for a would-be hacker.

"What is your pet's name?" Chances are that information has been mentioned on a Facebook timeline. "What is your mother's maiden name?" If not mentioned on a social media, an alarming amount of data is available on genealogy sites, such as ancestry.com. "What high school did you go to?" A picture of a recent reunion might be available on Instagram. And so on, and so forth.

However, even if someone shuns social media and never posts a single thing about themselves on the internet, that does not protect their answers to KBA "secret" questions. In December 2016, Yahoo revealed that in August 2013, it was the victim of the world's largest ever cyber-attack involving the breach of more than one billion user accounts. The information stolen in that attack included names, telephone numbers, dates of birth, passwords, and security questions and answers. Given that they relied on static KBA questions, chances are high that the same answers could be used to gain access to the users' other accounts that used static KBA questions.

I'M FORCED TO USE KBA, WHAT NOW?

As proven time and time again, passwords and security questions/answers are not secure, which has security experts advocating for the demise of KBA much in the same manner they have been for passwords. In fact, the federal government has taken steps to remove the question and answer KBA for federal accounts. Earlier this year, the National Institute of Standards and Technology ("NIST") released updated Digital Identity Guidelines. NIST indicated that it removed insecure authenticators from its recommended list, and security questions and answers are no longer endorsed as a protective measure.

A full transition away from question and answer KBA will not be simple or quick. However, in the meantime, there are some steps users can take now to strengthen security when using KBA.

- *Do not reuse the same security question*. A KBA question selected for one account should never be used as a KBA question for another account. Doing so just makes you more vulnerable in the event of a data breach.
- *Use unexpected answers to security questions*. If an online account, such as a bank or medical provider, continues to require question and answer KBA, do not answer the questions with the actual answers. This is especially true if the user previously had a Yahoo account at any point in the past due to their huge data breach. Generally speaking, security

questions only have one correct answer, which users are likely already using. How can you change these static answers? Simple—use a string of random characters. What is your pet's name? "BfQ27~9!" Where did you get married? "jptnY624&L" Again, these should not be repeated across accounts.

- *Use two-factor authentication*. Where available, make sure two-factor authentication is enabled to access your accounts. Authentication types are typically grouped into three categories: knowledge (i.e., something you know), possession (i.e., something you have), and inherence (i.e., something you are). KBA is based on knowledge. Authentication based on possession requires you to physically possess something else to authenticate your identity. Inherence uses biometric based authentication, such as fingerprint or retina scans. Two-factor authentication requires two steps to authenticate a user's identity, each step from a different category. For example, Google has the option of two-factor authentication when you sign in to a Google account. After inputting a password ("things you know"), Google will send a text message to the user's phone with a time-limited code ("things you have") that the user will then need to enter. Therefore, even if a hacker has a password, the hacker will not be able to gain access to the account if the hacker does not have the user's phone.

CONCLUSION

KBA can be a valuable tool against fraud, but to what degree ultimately falls on those corporations and financial institutions which rely on KBA as an authentication mechanism. If your company relies on KBA, make sure your company is taking the appropriate identity proofing measures when it comes to using KBA, such as using dynamic KBA questions rather than static KBA questions, pairing KBA with other identity verification technologies, etc.