The Banking Law Journal

Established 1889

An A.S. Pratt™ PUBLICATION **NOVEMBER/DECEMBER 2021**

LexisNexis

THE BANKING LAW JOURNAL

VOLUME 138 **NUMBER 10** **November/December 2021**

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)
ISSN: 0005-5506 (Print)

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.

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

MATTHEW BENDER

(2021–Pub.4815)

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 inquiries 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, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to bankers, officers of financial institutions, and their attorneys. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only 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.

Legal Impact of FFIEC Update to Authentication Guidance for Internet-Based Financial Services

Scott R. Fryzel, Lindsay S. Henry, and Lauren E. Quigley*

The Federal Financial Institutions Examination Council recently issued new guidance on risk management principles for access to and authentication of electronic funds transfers for the first time in over a decade. The authors of this article discuss the legal impact of the former guidance on the issue and what to expect from the new guidance.

The Federal Financial Institutions Examination Council (the "FFIEC") recently issued new guidance on risk management principles for access to and authentication of electronic funds transfers for the first time in over a decade, titled Authentication and Access to Financial Institution Services and Systems (the "New Guidance").[1] The New Guidance effectively replaces the FFIEC's prior guidance on this topic, including its original guidance issued in 2005, Authentication in an Internet Banking Environment (the "Original Guidance"), and the supplement issued in 2011 in response to increased fraud in internet-based financial transactions (the "Supplement,"[2] and together with the Original Guidance, the "Guidance"). The Guidance was intended to set regulatory expectations for financial institutions offering internet-based financial services to both commercial and consumer customers.

Supervisory guidance from financial institution regulators is generally viewed as establishing "best practices," but it does not have the force of law. However, courts have relied upon the Guidance in analyzing whether a bank's security procedures are commercially reasonable, which can be relevant in determining which party is ultimately liable and responsible for an unauthorized transaction. This legal precedent means that the Guidance, if followed, could mitigate risks and protect banks from losses and liability for unauthorized transactions. We expect that the New Guidance will continue to be relied upon by courts, and recommend that institutions review and incorporate the New Guidance into their operations, policies, and procedures going forward.

---

* Scott R. Fryzel (sfryzel@dykema.com) is a member in Dykema Gossett PLLC's Banking and Financial Services Group. Lindsay S. Henry (lhenry@dykema.com) and Lauren E. Quigley (lquigley@dykema.com) are both senior counsel in the firm's Banking and Financial Services Group.

[1] FFIEC 2021 Guidance, https://www.ffiec.gov/press/PDF/Authentication-and-Access-to-Financial-Institution-Services-and-Systems.pdf.

[2] FFIEC 2011 Supplement, https://www.fdic.gov/news/press-releases/2011/pr11111a.pdf.

ESTABLISHING COMMERCIALLY REASONABLE SECURITY PROCEDURES UNDER THE UCC

Courts have relied upon the Guidance in determining whether the security procedures agreed upon and used by financial institutions and their customers were commercially reasonable for purposes of authentication of payment orders as required by Article 4A of the Uniform Commercial Code ("UCC").[3] The standards established in the Guidance have been viewed by courts as commercially reasonable, and in cases where it was determined that a bank's security procedures were commercially reasonable and the bank accepted a payment order in good faith, the result was that the customer, and not the bank, should be responsible for the unauthorized transaction at issue.

An often cited case for this analysis is *Choice Escrow and Land Title, LLC v. BancorpSouth Bank* ("*Choice Escrow*").[4] In *Choice Escrow*, the court held that the loss of funds from the customer's account due to electronic fraud was the responsibility of the plaintiff customer, in part because the security procedures implemented by the defendant depository bank and agreed to by the customer were commercially reasonable.

In analyzing whether the security procedures were commercially reasonable, the court relied upon the Original Guidance as the "primary authority."[5] The *Choice Escrow* court noted requirements in the Original Guidance for the use of multi-factor authentication, and for banks to adjust their information security programs as unauthorized access threats evolve and change.[6] So while multi-factor authentication alone may have been inadequate in this instance, BancorpSouth had responded to new threats by offering its customers layered security in the form of "dual control." If customers refused dual control, as the plaintiff had, those customers were required to sign a waiver acknowledging that a single user would be permitted to originate and authorize electronic payment orders and funds transfers.

The court recognized that BancorpSouth had complied with the Original Guidance, including expanding security procedures into multi-layered procedures, and that its security procedure standards were generally followed by similarly-situated banks. This satisfied one prong of the court's analysis of whether BancorpSouth's security procedures were commercially reasonable; the

---

[3] UCC Section 4A-202.

[4] 754 F.3d 611 (8th Cir. 2014).

[5] *Id.* at 619.

[6] *Id.* at 620.

second prong of the analysis was that the security procedures were agreed upon with the customer based upon the customer's wishes expressed to the bank. The *Choice Escrow* court's analysis provided a blueprint for institutions to implement and offer security procedures, as well as how to document the adoption or rejection of those procedures by customers.

Essgekay Corp. v. TD Bank, N.A. ("*Essgekay*")[7] is another example of a court relying on the Guidance for its UCC analysis. The *Essgekay* court acknowledged the similarities between its state's version of UCC Article 4A and other states' versions, and how courts in other states have applied the Guidance when analyzing the commercial reasonableness of a bank's security procedures, citing *Choice Escrow* and another earlier case, *Patco Construction Co., Inc. v. People's United Bank*.[8] The *Essgekay* court held concisely that TD Bank required multi-factor authentication for the origination of electronic payment orders as required by the Guidance and thus its security procedures were commercially reasonable.

Similarly, the court in *Fed. Ins. Co. v. Benchmark Bank* ("*Benchmark*")[9] agreed that the multi-factor authentication system offered by the bank was commercially reasonable based upon its compliance with the requirements of the Guidance. The *Benchmark* court further analyzed whether the bank had offered the customer additional or alternative security procedures that would also be viewed as commercially reasonable and whether the customer had opted out of the use of those layered security procedures, as described in the Supplement.

In this instance, the customer had declined the implementation of additional security procedures, and the customer's decision to decline these layered security procedures was documented in an email from the customer to the bank. The customer had also agreed in writing to be bound by payment orders, whether or not authorized, made in the customer's name and accepted by the bank in compliance with the security procedures chosen by customer, whether or not such payment orders were authorized.[10]

Most recently, the court in *Rodriguez v. Branch Banking & Trust Co.*[11] followed the opinions of the courts in the *Benchmark* and *Patco Construction* cases in finding that the multi-factor authentication offered by the bank established a commercially reasonable security procedure in accordance with the requirements of the Supplement.

---

[7] 2018 U.S. Dist. LEXIS 214691 (D.N.J. 2018).

[8] 684 F.3d 197 (1st Cir. 2012).

[9] 2018 U.S. Dist. LEXIS 11152 (S.D. Ohio 2018).

[10] *Id.*

[11] 2021 U.S. Dist. LEXIS 63606 (S.D. Fla. 2021).

Based on these decisions, we have advised our clients to document the security procedures agreed upon with their commercial and consumer customers that originate electronic payment orders in order to demonstrate compliance with the Guidance. Most institutions already offer security procedures that are consistent with the requirements of the Guidance related to multi-factor authentication. But in many instances, banks are not obtaining written waivers from customers that refuse to follow the bank's recommended security procedure. Thus, it is important for banks to implement a process for obtaining such waivers in order to demonstrate their compliance with the Guidance.

THE NEW GUIDANCE—RISK ASSESSMENTS AND LAYERED SECURITY

The FFIEC stated that its primary reason for issuing the New Guidance, in addition to the increased threat landscape, is that financial institutions today are offering additional digital access points to use internet-based financial services that may result in unauthorized transactions. The FFIEC therefore recommends that institutions conduct a risk assessment of their digital banking and payments services to evaluate those risks, threats, vulnerabilities and controls associated with access and authentication, and offer the appropriate level of layered security procedures to their customers based on the risks identified.

Specifically, the New Guidance expands upon the scope and requirements of the Supplement by:

- Recognizing that authentication requirements are not only for customers, but also for employees, directors, and other third parties that use the bank's services and systems;
- Emphasizing the importance of a financial institution's risk assessment to determine appropriate access and authentication practices for the wide range of users; and
- Directing the need for layered security in authentication, of which multi-factor authentication is a part, but not the only security procedure offered or implemented for certain high-risk customers as identified by the institution's risk assessment.

The New Guidance provides examples of effective risk assessment practices and emphasizes the need to conduct risk assessments before introducing new financial services or access channels, as well as on a periodic basis to monitor evolving risks. The FFIEC explains that effective risk management practices will vary among institutions based upon their risk assessment findings, risk appetites and operational and technological complexity. Whether an institution offers and recommends the layering of security procedures, and the types of these

security procedures, should be determined based upon that institution's risk assessment findings and the particular access channel and user involved (i.e., customer, employee or third party). The New Guidance also includes a lengthy appendix with examples of practices and controls related to access management, authentication and supporting controls.

REVIEW AND UPDATE THE POLICIES AND PROCEDURES FOR CUSTOMER ADOPTION OR WAIVER OF SECURITY PROCEDURES

Consistent with the New Guidance, financial institutions are encouraged to document the risk assessment undertaken when deciding upon the security procedures offered and recommended to its commercial and consumer customers. Banks must also document their procedures for recommending and implementing authentication methods for the different types of customer access points (e.g., online, mobile, call center or help desk).

Often times a bank will implement security procedures that it issues to customers (e.g., tokens or passwords), but the bank does not have a written record or procedure documenting what security procedures were offered to the customer, including any layered security options that are available—for example, dual control and transaction limits are the most common procedures we see offered to customers for electronic funds transfers. These options should be provided or available in writing or online for review by customers so the bank will have documentation for purposes of demonstrating its compliance with the New Guidance.

The decision to permit waivers of any or all security procedures should be established by an institution's risk management team after careful consideration. In the event that multi-factor authentication and layered security options are offered to and refused by a customer, financial institutions should maintain a record of the customer's waiver or refusal of the security option. Any waiver terms should clearly state that the procedure was offered and recommended by the institution but the customer has refused the procedure, acknowledging the potential additional risk of proceeding without the procedure.

Banks will frequently offer layered security options such as transaction or daily limits in set-up or implementation forms for a particular service. If a customer will be permitted to waive a security option by virtue of their elections on a set-up or implementation form, that form should contain waiver terms and the customer should sign it to memorialize their waiver. These forms should not be signed or forwarded on solely by a bank employee, as that will not accomplish the ultimate goal of obtaining a written waiver executed by the customer.

As noted in the *Choice Escrow* and *Benchmark* cases, obtaining a waiver demonstrates the security procedure that was agreed upon with the customer after they refused the procedure offered and recommended by the bank, in order to meet the "commercially reasonable" standard under UCC Article 4A.

CONCLUSION

As the Guidance and case law makes clear, financial institutions that permit origination of payment orders without commercially reasonable security procedures run the risk of being liable for unauthorized transfers, unless the customer's written acknowledgement waiving such security procedures is obtained. The Guidance has been relied upon by courts to establish legal precedent as described above and we expect that the New Guidance will receive the same treatment going forward. As a result, banks should review and follow the New Guidance as it can provide a significant risk mitigant and protect banks from losses and liability for unauthorized transactions.