The Banking Law Journal

Established 1889

An A.S. Pratt™ PUBLICATION **JUNE 2019**

LexisNexis

THE BANKING LAW JOURNAL

VOLUME 136 **NUMBER 6** **June 2019**

LexisNexis®

UCC Section 4A-207(b) in the Age of Cybercrime

Benjamin W. Clements*

Section 4A-207(b) of the Uniform Commercial Code remains a potent tool for banks that find themselves involved in litigation simply because they processed a routine wire transfer. The author of this article discusses the provision and two recent cases that illustrate why Section 4A-207(b) is uniquely suited to protect banks involved in litigation arising out of email spoofing and compromise schemes.

In the age of cybercrime, financial institutions should remember the protections provided by Article 4A of the Uniform Commercial Code ("UCC"). Section 4A-207(b), in particular, remains a potent tool for banks that find themselves involved in litigation simply because they processed a routine wire transfer. That provision creates a "safe harbor" for banks that implement automated systems for processing funds transfers. In short, to realize economies of operation and reduce the potential for human error, the drafters of the UCC sought to incentivize banks to adopt such systems, and in Section 4A-207(b) they authored a rule beneficial to banks that do so. As two recent cases illustrate, Section 4A-207(b) is uniquely suited to protect banks involved in litigation arising out of the newest iteration of wire fraud in the evolving landscape of cybercrime—namely, email spoofing and compromise schemes.

SPOOFING AND E-MAIL COMPROMISE SCHEMES

There recently has been an alarming surge in email compromise activity worldwide. According to the Federal Bureau of Investigation's ("FBI") Internet Crime Complaint Center, commonly referred to as the IC3, cybercrime has become a billion-dollar industry and continues to grow steadily.[1] In 2015, the IC3 recorded $1.07 billion in reported losses from cybercrime.[2] In 2016, the

---

* Benjamin W. Clements is an associate in TroyGould PC's Litigation Department focusing on business and commercial litigation. He may be reached at bclements@troygould.com.

[1] Established in 2000, the IC3 receives complaints of Internet crime and produces annual reports to aggregate and highlight data provided by the general public for investigative, law enforcement, and public awareness purposes. FBI, Internet Crime Complaint Center (IC3), *2017 Internet Crime Report*, at 4, *available at* https://www.ic3.gov/media/annualreports.aspx. The IC3 has not yet released its annual report for 2018.

[2] FBI, IC3, *2015 Internet Crime Report*, at 12.

figure rose to $1.33 billion.[3] In 2017, it was $1.42 billion.[4] Nearly half the losses reported in 2017 resulted from a variation of the email compromise scheme, prompting the IC3 to begin tracking these scams as a single type of crime.[5] As of May 2018, global losses caused by business email compromise schemes reached $12.5 billion.[6] This is more than double the global losses of $5.3 billion reported as of December 2016, just 16 months earlier.[7]

E-mail compromise schemes generally involve the hacking or spoofing of a legitimate email address in order to induce the recipient of an email to wire funds to the fraudster's bank account.[8] Typically, the fraudster sends an email containing wire instructions to an individual who already intends to execute a funds transfer in furtherance of a business or consumer transaction. If the email does not raise suspicions, and the target does not confirm the instructions through another method of communication, the result is often that the email's recipient executes the funds transfer according to the email's instructions, only to discover the fraud after the fraudster removes the funds from the identified account.

Although these schemes usually follow this template, they are constantly evolving. Fraudsters are becoming more sophisticated and less discriminating, and they increasingly take time to research their marks before sending an initial email.[9] Demographic data shows scammers target persons of all age groups.[10]

---

[3] FBI, IC3, *2016 Internet Crime Report*, at 14.

[4] FBI, IC3, *2017 Internet Crime Report*, at 17.

[5] *2017 Internet Crime Report*, at 12 ("Because the techniques used in the BEC and EAC scams have become increasingly similar, the IC3 began tracking these scams as a single crime type in 2017."), 21 (attributing $676,151,185 in 2017 losses to BEC/EAC). The IC3 has highlighted the increasing prevalence and sophistication of email compromise schemes since 2014. *See 2014 Internet Crime Report*, at 16; *2015 Internet Crime Report*, at 10–11; *2016 Internet Crime Report*, at 9; *2017 Internet Crime Report*, at 12.

[6] FBI, Public Service Announcement (Alert No. I-071218-PSA), *Business E-mail Compromise The 12 Billion Dollar Scam* (July 12, 2018), https://www.ic3.gov/media/2018/180712.aspx (as of Feb. 27, 2019).

[7] FBI, Public Service Announcement (Alert No. I-050417-PSA), *Business E-mail Compromise E-Mail Account Compromise The 5 Billion Dollar Scam* (May 4, 2017), https://www.ic3.gov/media/2017/170504.aspx (as of Feb. 27, 2019).

[8] *See* FBI, Scams & Safety, Common Fraud Schemes, Internet Fraud, https://www.fbi.gov/scams-and-safety/common-fraud-schemes/internet-fraud (as of Feb. 27, 2019); *see also Medidata Sols., Inc. v. Fed. Ins. Co.*, 268 F. Supp. 3d 471, 477 n.2 (S.D.N.Y. 2017) ("Spoofing" is "'the practice of disguising a[n] . . . e-mail to make the e-mail appear to come from an address from which it actually did not originate.'").

[9] *2017 Internet Crime Report*, at 12.

Victims now include not only CEOs and CFOs but also less sophisticated actors, including individuals simply looking to buy their first home.[11] Indeed, from 2015 to 2017 alone, email compromise schemes targeting the real estate sector increased by more than 1,100 percent, causing a nearly 2,200 percent increase in reported monetary loss.[12]

In this country, California remains the principal target of these schemes. Since 2014, California has reported more complaints of cybercrime and greater total losses than any other state.[13] In 2016, for example, California had nearly double the number of cybercrime victims as the next closest state (Texas),[14] and more than double the total losses of the next closest state (New York).[15] In 2017, California again experienced nearly double the number of victims and amount of losses as the number two states for those categories (Florida and Texas, respectively).[16] Fortunately for financial institutions sued in California

---

[10] *See 2014 Internet Crime Report*, at 9 (9,442 complaints by persons under 20; 104,999 complaints by persons 20–39; 110,341 complaints by persons 40–59; 44,640 complaints by persons 60 and over); *2015 Internet Crime Report*, at 13 (10,435 victims under 20; 51,302 victims age 20–29; 57,019 victims age 30–39; 58,253 victims age 40–49; 59,128 victims age 50–59; 51,875 victims age 60 and over); *2016 Internet Crime Report*, at 14 (10,004 victims under 20; 46,266 victims age 20–29; 54,670 victims age 30–39; 51,394 victims age 40–49; 49,208 victims age 50–59; 55,043 victims age 60 and over); *2017 Internet Crime Report*, at 17 (9,053 victims under 20; 41,132 victims age 20–29; 45,458 victims age 30–39; 44,878 victims age 40–49; 43,764 victims age 50–59; 49,523 victims age 60 and over).

[11] *See 2017 Internet Crime Report*, at 12 (describing evolution of email compromise schemes); *see, e.g.*, *Thuney v. Lawyer's Title of Ariz.*, No. 2:18-cv-1513-HRH (D. Ariz. Feb. 6, 2019) (plaintiffs seeking to buy retirement home sued, among others, bank of beneficiary of fraudulent wire transfer); *Bain v. Cont'l Title Holding Co.*, No. 16-2326-JWL (D. Kan. Jan. 20, 2017) (homebuyers sued, among others, bank that transferred funds due to email compromise scheme).

[12] FBI, Public Service Announcement (Alert No. I-071218-PSA), *Business E-mail Compromise The 12 Billion Dollar Scam* (July 12, 2018), https://www.ic3.gov/media/2018/180712.aspx (as of Feb. 27, 2019); Schwartz, Mathew J., *FBI: Global Business Email Compromise Losses Hit $12.5 Billion*, BANKINFO SECURITY (July 16, 2018), https://www.bankinfosecurity.com/fbi-alert-reported-ceo-fraud-losses-hit-125-billion-a-11206 (as of Feb. 27, 2019); Egan, Gretel, *$12.5 Billion Lost in BEC Attacks, FBI Reports*, PROOFPOINT (July 25, 2018), https://www.wombatsecurity.com/blog/12.5-billion-lost-in-bec-attacks-fbi-reports (as of Feb. 27, 2019).

[13] *See 2014 Internet Crime Report*, at 20–21 (Appendix I), 25 (Appendix II) (30,923 complaints; $131,363,796 in losses); *2015 Internet Crime Report*, at 14, 17–18, 38 (34,842 complaints; $195,490,403 in losses); *2016 Internet Crime Report*, at 16, 19–20 (39,547 victims; $255,181,657 in losses); *2017 Internet Crime Report*, at 19, 22–23 (41,974 victims; $214,217,307 in losses).

[14] *2016 Internet Crime Report*, at 19.

[15] *Id.* at 20.

[16] *2017 Internet Crime Report*, at 22–23.

by victims of cybercrime, California has adopted Article 4A as division 11 of the California Uniform Commercial Code, thereby incorporating its protections into California state law.[17]

These protections remain effective tools for banks involved in litigation arising out of new forms of wire fraud.[18] One such protection—the safe harbor provided by Section 4A-207(b)—has recently proven effective where the wire fraud concerns spoofing or an email compromise scheme. And, like California, every other state in the union has enacted Section 4A-207(b) in one form or another.[19]

---

[17] *See Zengen, Inc. v. Comerica Bank*, 158 P.3d 800, 804 (Cal. 2007).

[18] *See, e.g.*, *First Sec. Bank of New Mexico, N.A., v. Pan Am. Bank*, 215 F.3d 1147, 1154–55 (10th Cir. 2000) (reversing summary judgment due to factual issues whether bank—whose employees reviewed wire transfers—had "actual knowledge" of discrepancy between beneficiary account number and named beneficiary); *Greenfield v. Tassinari*, 8 A.D.3d 529, 533 (N.Y. App. Div. 2004) (affirming summary judgment in favor of banks that "submitt[ed] evidence that the funds were transferred through a fully automated electronic system and were credited to the account numbers provided in the transfer instructions"); *TME Enterprises, Inc. v. Norwest Corp.*, 22 Cal. Rptr. 3d 146, 156 (Ct. App. 2004) (affirming judgment in favor of bank because substantial evidence supported finding that bank—with partially automated system calling for some human involvement—did not have "actual knowledge" of discrepancy between account number and name); *Zengen, Inc. v. Comerica Bank*, 158 P.3d 800, 807-08 (Cal. 2007) (analyzing the ways division 11 of California Uniform Commercial Code displaces common law claims); *Sliders Trading Co. v. Wells Fargo Bank NA*, No. 17-cv-04930-LB (N.D. Cal. Dec. 21, 2017) (granting bank's 12(b)(6) motion to dismiss because section 11207 of California Uniform Commercial Code displaced negligence claim); *Peter E. Shapiro, P.A. v. Wells Fargo Bank, N.A.*, 352 F. Supp. 3d 1226, (S.D. Fla. Nov. 5, 2018) (granting bank's summary judgment motion because Section 670.207 of Florida Statutes preempted negligence claim and bank's automated system processed wire transfer).

[19] Ala. Code § 7-4A-207(b); Alaska Stat. § 45.14.207(b); Ariz. Rev. Stat. Ann. § 47-4A207(B); Ark. Code Ann. § 4-4A-207(b); Cal. Com. Code § 11207(b); Colo. Rev. Stat. Ann. § 4-4.5-207(b); Conn. Gen. Stat. Ann. § 42a-4A-207(b); Del. Code Ann. tit. 6, § 4A-207(b); D.C. Code § 28:4A-207(b); Fla. Stat. Ann. § 670.207(2); Ga. Code Ann. § 11-4A-207(b); Haw. Rev. Stat. § 490:4A-207(b); Idaho Code Ann. § 28-4-615(2); 810 Ill. Comp. Stat. Ann. 5/4A-207(b); Ind. Code Ann. § 26-1-4.1-207(b); Iowa Code Ann. § 554.12207(2); Kan. Stat. Ann. § 84-4a-207(b); Ky. Rev. Stat. Ann. § 355.4A-207(2); La. Rev. Stat. Ann. § 4A-207(b); Me. Rev. Stat. Ann. tit. 11, § 4-1207(2); Md. Code Ann., Com. Law § 4A-207(b); Mass. Gen. Laws Ann. ch. 106, § 4A-207(b); Mich. Comp. Laws Ann. § 440.4707(2); Minn. Stat. Ann. § 336.4A-207(b); Miss. Code Ann. § 75-4A-207(b); Mo. Ann. Stat. § 400.4A-207(b); Mont. Code Ann. § 30-4A-207(2); Neb. Rev. Stat. Ann. § 4A-207(b); Nev. Rev. Stat. Ann. § 104A.4207(2); N.H. Rev. Stat. Ann. § 382-A:4A-207(b); N.J. Stat. Ann. § 12A:4A-207(2); N.M. Stat. Ann. § 55-4A-207(b); N.Y. U.C.C. Law § 4-A-207(2); N.C. Gen. Stat. Ann. § 25-4A-207(b); N.D. Cent. Code Ann. § 41-04.1-15(2); Ohio Rev. Code Ann. § 1304.62(B); Okla. Stat. Ann. tit. 12a, § 4A-207(b); Or. Rev. Stat. Ann. § 74A.2070(2); 13 Pa. Const. Stat. Ann. § 4A207(b); R.I. Gen. Laws Ann. § 6A-4.1-207(b); S.C. Code Ann. § 36-4A-207(b);

SECTION 4A-207(b)

Section 4A-207(b) may immunize banks that use automated systems to process wire transfers. In the schemes described above, fraudulent email instructions generally identify the transfer's beneficiary by name and account number. Although the email correctly names the intended beneficiary, it supplies the number of an account under the fraudster's control. Upon seeing the correct name, the recipient often forwards the instructions to his or her own financial institution to initiate the transfer. Section 4A-207(b) creates a safe harbor for the beneficiary's bank that processes the transfer by looking to the account number without regard to the name.[20] Under Section 4A-207(b), "[i]f a payment order received by the beneficiary's bank identifies the beneficiary both by name and by an identifying or bank account number and the name and number identify different persons," the bank "need not determine whether the name and number refer to the same person."[21] Instead, "if the beneficiary's bank does not know that the name and number refer to different persons, it may rely on the number as the proper identification of the beneficiary of the order."[22]

In these cases, the liability of the beneficiary's bank turns on whether the bank, at the time of payment, had "actual knowledge" that the identified number did not correspond to the name of the identified beneficiary.[23] Banks rarely should have actual knowledge of such a discrepancy. As the Official Comments to Section 4A-207(b) recognize, "A very large percentage of payment orders . . . are processed by automated means using machines . . . that identify the beneficiary by an identifying number or the number of a bank account. The processing of the order . . . and the crediting of the beneficiary's account are done by use of the identifying or bank account number without human reading of the payment order itself."[24]

The safe harbor afforded by Section 4A-207(b) reflects a policy decision to encourage banks to prioritize efficiency by executing transfers via automated

---

S.D. CODIFIED LAWS § 57A-4A-207(b); TENN. CODE ANN. § 47-4A-207(b); TEX. BUS. & COM. CODE ANN. § 4A.207(b); UTAH CODE ANN. § 70A-4a-207(2); VT. STAT. ANN. tit. 9A, § 4A-207(b); VA. CODE ANN. § 8.4A-207(b); WASH. REV. CODE ANN. § 62A.4A-207(b); W. VA. CODE ANN. § 46-4A-207(b); WIS. STAT. ANN. § 410.207(2); WYO. STAT. ANN. § 34.1-4.A-207(b).

[20] *TME Enterprises, Inc. v. Norwest Corp.*, 22 Cal. Rptr. 3d 146, 153 (Ct. App. 2004).

[21] U.C.C. § 4A-207(b)(1).

[22] *Id.*

[23] Official Comment No. 2 to U.C.C. § 4A-207.

[24] *Id.*

means. The Official Comments to the rule explain that imposing a duty on banks to determine whether the name and number refer to the same person means sacrificing the benefits of automated payment. "Manual handling of payment orders is both expensive and subject to human error. If payment orders can be handled on an automated basis there are substantial economies of operation and the possibility of clerical error is reduced."[25] This policy decision is at the heart of the rule and reinforces why Section 4A-207(b) can be such a potent defense for banks that become embroiled in wire fraud litigation, particularly where the genesis of the suit is spoofing or email compromise activity.

Indeed, two recent cases illustrate that Section 4A-207(b) remains a powerful tool for banks to extricate themselves from litigation arising out of spoofing and email compromise schemes. These are a December 2017 case in the Northern District of California and a November 2018 case in the Southern District of Florida.

SLIDERS TRADING CO. v. WELLS FARGO BANK N.A.

In December 2017, the U.S. District Court for the Northern District of California held that Section 11207(b) of the California Uniform Commercial Code barred the claims asserted by a victim of an email compromise scheme against Wells Fargo.[26] In *Sliders Trading Co. v. Wells Fargo Bank N.A.*, a fraudster fooled Sliders Trading Co. into believing it was a long-time business partner—a California company named Grow More, Inc.—by spoofing Grow More's domain names and email addresses.[27] Certain emails provided wire instructions naming "Grow More of 15600 New Century Drive, Gardena, California 90248" as beneficiary and identifying a Wells Fargo account number.[28] Believing Grow More had authored the emails, Sliders Trading wired more than $500,000 to the identified account.[29] When additional emails revealed the

---

[25] *Id.*; *see also TME Enterprises, Inc. v. Norwest Corp.*, 22 Cal. Rptr. 3d 146, 158 (Ct. App. 2004) ("'If it is not true already, soon the entire transaction—after it has been mechanically entered into the system—will be completed without the intervention of human eyes or hands. Presumably, therefore, machines will be instructed to read the numbers and to credit the amount represented by the numbers in the numbered account in complete obliviousness to the name on the account.'").

[26] *Sliders Trading Co. v. Wells Fargo Bank NA*, No. 17-cv-04930-LB (N.D. Cal. Dec. 21, 2017).

[27] *Id.*

[28] *Id.*

[29] *Id.*

fraud, Sliders unsuccessfully attempted to recover the wired funds and then sued Wells Fargo for negligence.[30]

Wells Fargo moved to dismiss the complaint under FRCP 12(b)(6), arguing that Section 11207(b) displaced the negligence claim and "otherwise provides immunity to Wells Fargo via its safe-harbor provision."[31] The court granted the motion with leave to amend, holding that Section 11207(b) displaced (or preempted) the common law claim for negligence.[32] Under California law, division 11 of the California Uniform Commercial Code "'displaces other common law remedies and claims for relief (1) where the common law claims would create rights, duties, or liabilities inconsistent with division 11; and (2) where the circumstances giving rise to the common law claims are specifically covered by the provisions of division 11.'"[33] Because the negligence claim alleged that the wire instructions not only named Grow More as the beneficiary but also identified an account that did not belong to Grow More, the court concluded that Section 11207(b) "covers the circumstances of the fraud" and barred the common law claim.[34]

Notably, the court also rejected Sliders' argument that Wells Fargo should have noticed "red flags" surrounding the transactions. Among other things, Sliders sought to emphasize so-called "know your customer" laws, alleging that Wells Fargo "allowed one or more imposters to open at least *four* separate accounts in at least *three* separate states, each in the name of the same established California corporation."[35] In opposing the motion to dismiss, Sliders argued that "the gravamen of [its] claim is that Wells Fargo should not have given criminals repeated access to the banking system. . . ."[36] The court concluded that these arguments were an attempt to circumvent Section 11207(b). Sliders effectively sought to impose a duty on Wells Fargo to determine whether the name and number identified in the fraudulent emails referred to the same person, which would effectively impose liability for, at most, constructive knowledge of the discrepancy between the name and

---

[30] *Id.*

[31] *Id.*

[32] *Id.*

[33] *Id.* (quoting *Zengen, Inc. v. Comerica Bank*, 158 P.3d 800, 808 (Cal. 2007)).

[34] *Id.*

[35] First Amended Complaint, ECF No. 17 at ¶ 5, *Sliders Trading Co. v. Wells Fargo Bank NA*, No. 17-cv-04930-LB.

[36] Opposition to Motion to Dismiss, ECF No. 19 at 3:11–12, *Sliders Trading Co. v. Wells Fargo Bank NA*, No. 17-cv-04930-LB.

number. Such liability would have been inconsistent with Section 11207(b)'s actual knowledge requirement.

PETER E. SHAPIRO, P.A. v. WELLS FARGO BANK, N.A.

More recently, in November 2018, the U.S. District Court for the Southern District of Florida went a step further: After dismissing a negligence claim against Wells Fargo on the ground that Section 670.207 of the Florida Statutes preempted the claim, the court granted Wells Fargo's motion for summary judgment based on evidence that Wells Fargo processed the wire transfer via automated means.[37]

In *Peter E. Shapiro, P.A. v. Wells Fargo Bank, N.A.*, a law firm executed a $500,000 wire transfer on behalf of a client that was repaying a loan.[38] The client forwarded an email to the firm from the lender's attorney containing wire instructions, which identified an account at M & T Bank in New York.[39] The next day, the client forwarded a second email purporting to be from the lender's attorney that directed payment to a Wells Fargo account in Texas.[40] Neither the client nor the law firm questioned the change. And despite the two inconsistent sets of wire instructions, as well as typographical and capitalization errors in the second email, the law firm initiated the transfer to the Wells Fargo account.[41] When the law firm was unable to recover the funds, it sued Wells Fargo for negligence and a violation of Section 670.207.[42]

Wells Fargo moved for summary judgment on the ground that it processed the wire transfer through an automated, electronic system and therefore did not have actual knowledge of any discrepancy in the wire transfer instructions.[43] The bank submitted evidence that when instructions identify a valid Wells Fargo account number, its internal system processes the transfer through an automated system without human involvement.[44] Additionally, although bank personnel reviewed the transfer for possible U.S. sanctions violations, that

---

[37] *Peter E. Shapiro, P.A. v. Wells Fargo Bank, N.A.*, 352 F. Supp. 3d 1226, (S.D. Fla. Nov. 5, 2018).

[38] *Id.*

[39] *Id.*

[40] *Id.*

[41] *Id.*

[42] *Id.*

[43] *Id.*

[44] *Id.*

screening process did not concern a possible mismatch between the named beneficiary and the identified account.[45]

The court granted Wells Fargo's motion, holding that Section 670.207 "permits, and indeed encourages, banks to process electronic funds transfers via automated systems. Moreover, it expressly excuses banks from any duty to verify whether the recipient's name and the name on the receiving account match."[46] Because Wells Fargo processed the transfer via automated means, the court reasoned there was no evidence the bank had actual knowledge that the named beneficiary did not correspond to the identified account number.[47]

The *Shapiro* case demonstrates how difficult it can be to prove actual knowledge. Even though a bank employee set eyes on the wire information, because the purpose of that review was unrelated to the relationship between beneficiary name and account number, the act of reviewing the wire information was not sufficient evidence of actual knowledge to create a triable issue. Although "a person reviewed the transaction for sanctions compliance," the court noted, "the person did not look at whether the name and account number matched. At no point in the process did anyone become consciously aware that the name and account did not match."[48] The court concluded that the law firm could not "impose a duty of care upon Wells Fargo that the statute expressly rejects."[49]

CONCLUSION

These two cases demonstrate the variety of situations in which email compromise schemes occur and contexts in which banks are sued simply for processing routine wire transfers. The *Shapiro* case, in particular, shows that the ubiquity of email often means that fraudsters have more than one potential target in any given scheme and also opportunity to exploit less sophisticated actors or systems to the detriment of others involved in the same transaction. The result is that financial institutions—including the beneficiary's bank involved at the end of the transaction—are likely to continue to find themselves parties to litigation merely for implementing efficient systems for processing funds transfers. In this circumstance, banks should remember the protections provided by the drafters of the UCC and specifically those afforded by Section

---

[45] *Id.*

[46] *Id.*

[47] *Id.*

[48] *Id.*

[49] *Id.* An appeal of the *Shapiro* case is currently pending.

4A-207(b). These rules continue to govern the liability of those involved in funds transfers and, as *Sliders Trading* and *Shapiro* illustrate, are well suited to protect banks from claims involving spoofing or email compromise schemes, where the fraud often occurs well before the banks become involved.

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

(2019–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 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, 646.539.8300. 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.