

THE LEGAL ISSUE | MAY 2016

BankDirector®

GUIDED BY ONE PRINCIPLE: STRONG BOARDS BUILD STRONG BANKS

BATTLING HEDGE
FUND CONTROL

THE LEGAL ISSUE

TARGETING
OVERDRAFT FEES

FINES GET LARGER
AGAINST BANK
DIRECTORS

GETTING HACKED:
CURRENT
CYBERSECURITY
THREATS

HOW TO USE THE BANK DIRECTOR DIGITAL APP

Look for these icons throughout the issue to indicate interactivity.



Hotspots

Tap these icons to access interactive elements inside articles.



Play Video

Look for this icon to indicate a video. Tap to view the video inside the app.



Directional Swipe

Various icons instruct you to use a directional swipe to access additional information.



Way Finding

Look for this arrow icon to help you navigate through the issue's articles.



Internet Access

This icon indicates Internet access is required for interactive elements.

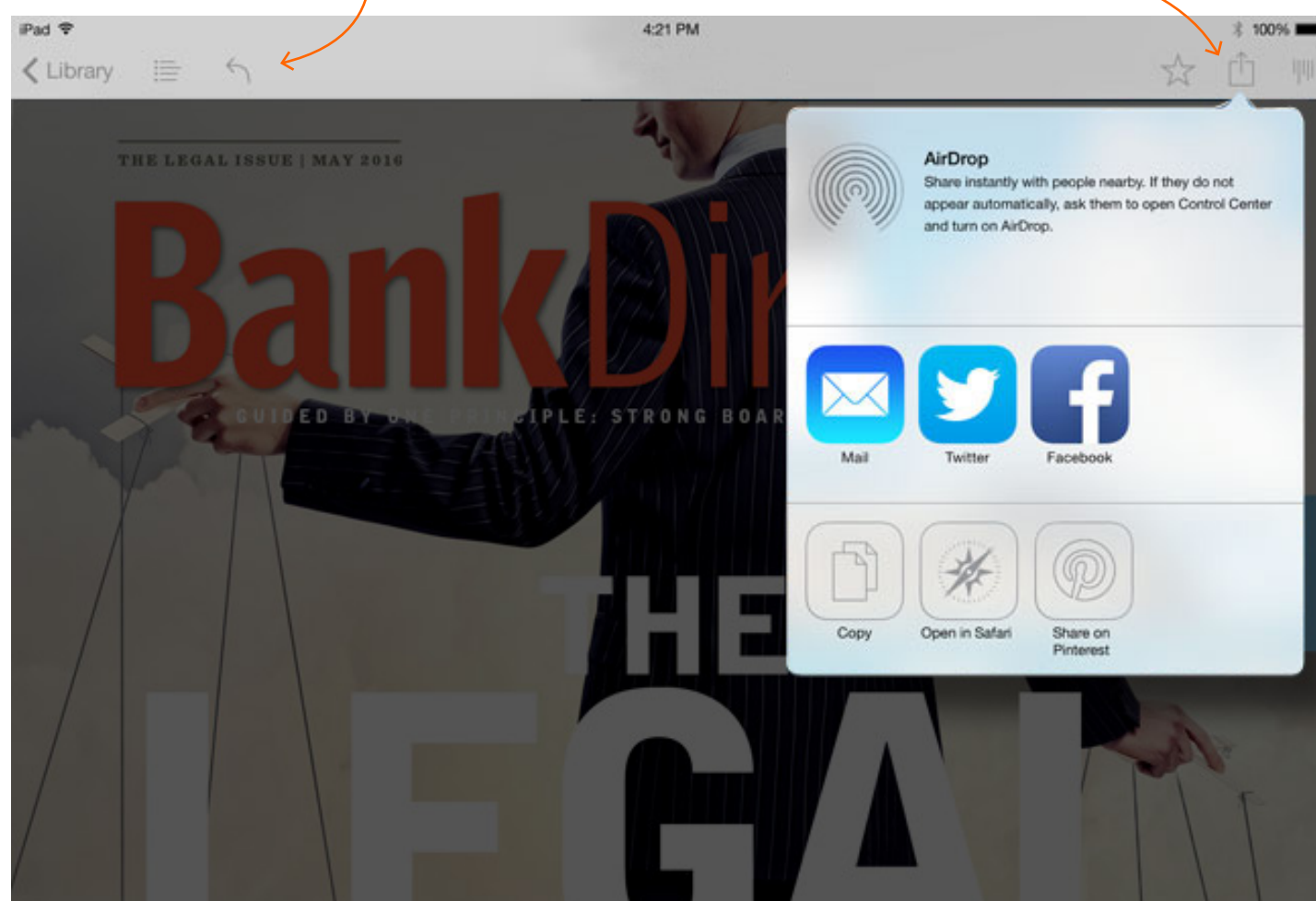
How to use the in-app toolbar.

Menu Bar

Tap the screen to quickly access the library of archived issues, back button and table of contents.

Social Sharing

When indicated, share an article by tapping a sharing button to access the toolbar. The sharing icon located in the top right gives you various social media platforms to share the article.



In-Print. In-Person. Online.

GUIDED BY ONE PRINCIPLE: STRONG BOARDS BUILD STRONG BANKS


DIGITAL MAGAZINE

THE LEGAL ISSUE CONTENTS



BATTLING HEDGE FUND CONTROL

Bank-related activism makes a comeback.

 *A Look at Hedge Fund Activists Who Target Banks*



LETTER FROM THE EDITOR

The world now emphasizes fairness for consumers.

BRIEFLY NOTED

A BOARDROOM CONVERSATION

Jim Chiafullo, a director at F.N.B. Corp., talks about unlocking shareholder value.

VIDEO

A conversation with Bank of the West Chairman J. Michael Shepherd.

INTERACTIVE POLL

Stay Connected



Like us on
Facebook



Follow
Bank Director
on LinkedIn



Follow
@BankDirector
on Twitter



Watch educational
videos on
Bank Director's
YouTube Channel

BANKDIRECTOR.COM

THE WORLD NOW EMPHASIZES FAIRNESS FOR CONSUMERS

The world is a better place for consumers. Whereas U.S. law previously emphasized disclosure as a way to protect consumers, changes in the law and its interpretation now emphasize fairness.

The most obvious example of this is the Consumer Financial Protection Bureau (CFPB), created nearly six years ago by the Dodd-Frank Act with the sole mission of looking after the interests of financial consumers. The CFPB did away with lengthy mortgage documents, primarily cobbled together by a series of previous laws that emphasized disclosure, with two simpler forms—the “Know Before You Owe” documents, which describe borrowers’ mortgages, and secondly, their closing expenses. Plus, consumers must receive their closing paperwork at least three days beforehand so they can review and ask questions. This was always something a consumer could ask for, but many people didn’t know they could demand it.

When I was covering the financial crisis in 2006 and 2007 for *The Tennessean*, a daily newspaper in Bank Director’s hometown of Nashville, I often interviewed homeowners who were struggling with subprime mortgages and seemed to have little understanding of their mortgages. One woman said her mortgage broker showed up at her hair salon with her closing documents pushing her to sign on her half-hour lunch break. When I asked one man if he



Naomi Snyder
is editor for
Bank Director.



Tap *below* to tell us what you think of the digital magazine.

✉ **Naomi Snyder** | nsnyder@bankdirector.com

THE WORLD NOW EMPHASIZES FAIRNESS FOR CONSUMERS

up at her hair salon with her closing documents pushing her to sign on her half-hour lunch break. When I asked one man if he had a fixed-rate or an adjustable-rate mortgage, he told me it was fixed, because it was fixed for three years. (After three years, his subprime rate adjusted to a new rate he couldn't afford unless he had won the lottery.)

This is not to say that everyone will understand their mortgages because they are explained in simpler terms. But the very tone of regulation has changed. As you can see in John Maxfield's story on overdrafts in this issue, the CFPB is pushing banks to not only offer, but also market, low-cost deposit accounts with no overdraft fees. Overdraft programs that are confusing to consumers are likely to get banks in trouble, and indeed, already have.

Additionally, several aspects of consumer law have been taken out of the hands of the prudential bank regulators and moved to the CFPB, which is totally focused on the task of consumer protection, not the safety and soundness of the banking system. Rule-making authority for the Home Mortgage Disclosure Act, for example, is now in the hands of the CFPB. Previously the Federal Reserve had that responsibility. The CFPB also is going after nonbanks. The agency has made it clear that payday lenders will be getting new regulations despite that industry's long



Naomi Snyder
is editor for
Bank Director.



Tap *below* to tell us what you think of the digital magazine.

✉ **Naomi Snyder** | nsnyder@bankdirector.com

THE WORLD NOW EMPHASIZES FAIRNESS FOR CONSUMERS

after nonbanks. The agency has made it clear that payday lenders will be getting new regulations, despite that industry's long history of complying with disclosure rules regulated by the various states. Disclosure, when it comes to payday loans, is clearly not enough to protect consumers in the CFPB's view.

There has been a lot of concern in the banking industry about what the new regulations might mean for banks. Many banks, especially small ones, are finding the new regulations onerous and some of them are even leaving consumer lending, particularly mortgages, altogether. I think we will see increased consolidation of mortgage lending to the big mortgage brokers and banks, because they can afford the cost of keeping up with regulations and still make such a business profitable, which will be unfortunate for many potential homeowners who won't fit in their underwriting check boxes of decent credit history and documented, regular income.

But despite obvious drawbacks such as these, the world is getting to be a much better place for consumers, and that's not so bad for banks, either. Banks who recognize this are positioning themselves to offer financial advice and contribute to the overall well being of their customers, not just push short-term transactions. Customers who can reduce debt and improve their financial well being can help the economy, and banks by starting



Naomi Snyder
is editor for
Bank Director.



*Tap **below** to tell us what you think of the digital magazine.*

✉ **Naomi Snyder** | nsnyder@bankdirector.com

THE WORLD NOW EMPHASIZES FAIRNESS FOR CONSUMERS

transactions. Customers who can reduce debt and improve their financial well being can help the economy, and banks, by starting their own businesses and managing their loans better. Better educated consumers making better financial decisions make better customers, too.



Naomi Snyder
is editor for
Bank Director.



*Tap **below** to tell us what you think of the digital magazine.*

✉ **Naomi Snyder** | nsnyder@bankdirector.com

◆

..... IT'S A

COMPLEX

..... FINANCIAL WORLD.

AND IT'S NOT.

At Vorys, our financial services practice is as sophisticated as you need it to be. We know how to handle all the complexities of the financial world. We also know how to be practical, straightforward and just get the job done. And we have developed a unique and effective interdisciplinary team approach to business that covers every facet of financial services

..... in a cost-effective manner.

LEARN MORE



VORYS

Higher standards make better lawyers.®

Vorys, Sater, Seymour and Pease LLP 52 East Gay Street, Columbus, Ohio 43215

Columbus

Washington

Cleveland

Cincinnati

Akron

Houston

Pittsburgh

The legal issues bank boards need to worry about keep increasing. Regulatory pronouncements are par for the course. But now, the CFPB is adding a few more to the mix. Take a look at the following upcoming legal and regulatory matters that could impact your bank, or its competitors.

Naomi Snyder
is editor for
Bank Director.

Tap the numbered icons to cycle through topics

1 2 3 4

CRE WARNING TO BANKS

Real estate has been a strong part of many regional economies, and commercial real estate is a real money maker for many community banks across the nation. In that context, regulators put out a warning shot last December in the form of **joint regulatory guidance**, stating that underwriting has been loosened in the commercial real estate sector, and CRE lending will be a focus for 2016 bank examinations. The reviews will focus on “financial institutions’ implementation

SWIPE UP



BATTLING HEDGE FUND CONTROL

BY JOHN ENGEN

Bank-related activism makes a comeback.

Shareholder activists have been running roughshod over corporate America in recent years, challenging boards to return capital to shareholders, cut costs, split their companies into pieces and even sell—all in the name of “unlocking hidden value” for shareholders. When boards don’t respond the right way, activists aren’t afraid to seek board seats.

Banks have been relatively immune to the trend. Post-financial crisis regulations, a tough operating environment and, significantly, the inability of investors to obtain a controlling position and force changes on bank boards without regu-

latory approval, have conspired to shield the industry from the activist frenzy.

Now, that appears to be changing. The industry is fundamentally healthier than it's been in a while, but many banks still aren't able to earn even the 9 percent on equity required to break even on capital costs. While the regulatory environment remains tough, the agencies seem more willing to approve strategic changes and mergers.

Activists launched 22 campaigns at banks in 2015—a number that has risen every year since the crisis, according to Thomson Reuters activism data. The number of activist encounters that don't result in proxy scuffles is even greater: In a survey by consultant PwC, 31 percent of financial institution directors say their boards interacted with activists in 2015, up from 23 percent the year before.

“Activism is increasing, and it's also moving up the food chain,” says Joseph Vitale, a partner at Schulte Roth & Zabel LLP, a New York law firm. “The sector has been distressed, and it's been experiencing low rates of returns. These are the kinds of situations where you expect to see activism.”

Richard Lashley, a principal of PL Capital, a hedge fund that owns shares in 38 banks, says that rising compliance and technology costs, combined with continued margin pressures spawned by the Federal Reserve's low-rate policies, have made the industry “ripe for activism.” Oftentimes, he says, the cost savings from a forced merger can be more than double the net income of the seller, making a sale “a no-brainer.”

Two banks where PL Capital held board seats—Metro Bancorp in Harrisburg, Pennsylvania, and Sioux Falls, South Dakota-based HF Financial Corp.—agreed last year to merge with larger institu-



22

Activists launched 22 campaigns at banks in 2015—a number that has risen every year since the crisis.

tions after feeling the heat. “Our thesis is that we’re returning to the days of acquire or be acquired. You could be a buyer or a seller, but clearly there’s a need for greater economies of scale,” Lashley says. “Everyone in the boardroom knows what needs to be done. Sometimes, they just need a nudge.”

“Companies that are providing good returns are not interesting to activists. If it ain’t broke, there’s nothing to fix.”

— JOSEPH VITALE, PARTNER, SCHULTE ROTH & ZABEL LLP

Activism isn’t exactly new to banking. Anyone who’s been around the industry awhile can recall the wave of activism—much of it connected to mutual thrift conversions—in the 1990s and early 2000s. A 2015 study by the Federal Reserve Bank of Kansas City found an average of 8.5 percent of publicly traded banks and thrifts had a publicly disclosed encounter with an activist in any given year between 1994 and 2010.

This new breed of activism has a sharper edge to it. Investors have more governance tools—proxy access, annual elections and required non-binding say-on-pay resolutions—at their disposal and aren’t shy about challenging for board seats if they don’t get their way. Sometimes they attack in packs to get around regulatory restrictions on control. Metro, which had \$3 billion in assets and 32 branches, sold to F.N.B. Corp. of Pittsburgh after three separate hedge funds—PL Capital, Basswood Capital and Clover Partners—all pressed for a deal.

While smaller banks have traditionally gotten most of the at-





You have goals.
We have **solutions.**
Let's talk.

BMO



**BMO Harris Bank
BMO Capital Markets**

BMO offers a wide selection of focused and specialized solutions, including interest rate and treasury management. As one of North America's largest financial institutions, we have the capabilities and experience to deliver exceptional service to our correspondent bank clients.

bmoharris.com/correspondent | bmocm.com

Banking products and services are provided by BMO Harris Bank N.A. Member FDIC. BMO Capital Markets is a trade name used by BMO Financial Group for the wholesale banking businesses of Bank of Montreal, BMO Harris Bank N.A. (member FDIC), Bank of Montreal Ireland p.l.c., and Bank of Montreal (China) Co. Ltd and the institutional broker dealer businesses of BMO Capital Markets Corp. (Member SIPC) in the U.S., BMO Nesbitt Burns Inc. (Member Canadian Investor Protection Fund) in Canada and Asia and BMO Capital Markets Limited (authorised and regulated by the Financial Conduct Authority) in Europe and Australia. "BMO Capital Markets" is a trademark of Bank of Montreal, used under license. "BMO (M-Bar roundel symbol)" is a registered trademark of Bank of Montreal, used under license. ® Registered trademark of Bank of Montreal in the United States, Canada and elsewhere.

tention from hedge funds that specialize in financial companies, activists are increasingly challenging larger institutions. Last October, the board of \$15.1 billion asset Astoria Financial Corp. in Lake Success, New York, agreed to have the bank acquired by rival New York Community Bancorp after activist Basswood Capital Management took a 9.2 percent stake and began agitating for a sale. In February, New York hedge fund Hudson Executive Capital announced stakes in \$48 billion asset CIT Group and Comerica Bank, a \$71 billion asset lender based in Dallas. It wants CIT to divest some units, and would like Comerica, which had a 7 percent year-end 2015 average return on equity, to sell.

Even megabanks are vulnerable. Last year, Trian Fund Management, a \$12 billion hedge fund run by billionaire Nelson Peltz, accumulated a 2.5 percent stake in Bank of New York Mellon Corp., and pressured its way onto the board. Trian, which invests in many different industries, has since grown its position to 2.83 percent of BNY Mellon shares.

Preparation is the key to avoiding or fending off an activist attack. A growing number of bank boards are hiring outside advisors to, in essence, pretend they are activists and review operations for vulnerabilities that might attract attention and can be addressed. “It could be anything from an operational deficiency to a lack of independence or skill on the board,” says Robert Klingler, a partner with law firm Bryan Cave in Atlanta. “It’s about anticipating what might happen and how you would respond.”

Some boards are identifying response teams of lawyers, investment bankers and directors who are ready to jump into action if an activist emerges. Many are reviewing their bylaws and articles of incorporation to make sure the proper defenses are in place. A growing number of institutions also are monitoring their share-



In a survey by consultant PwC, 31 percent of financial institution directors say their boards interacted with activists in 2015.

holder rolls more closely, and gaining perspective on how their largest shareholders have reacted to activist plays at other companies.

H. Rodgin Cohen, senior chairman of New York law firm Sullivan & Cromwell LLP, advises his clients to talk more often with larger shareholders whose voting support an activist needs to succeed. “You don’t want to talk just about last year’s performance, but also long-term strategy,” he says. “If an activist strikes, you can say to them, ‘As we’ve already told you, we have a good strategy.’ You want to take the initiative, rather than being on the defensive.” Bank boards appear to be taking such words to heart. In the PwC survey, 67 percent of financial institution directors reported communicating “regularly” with large shareholders.

Of course, the best way to hold activists at bay is to perform well. “Companies that are providing good returns are not interesting to activists,” Vitale says. “If it ain’t broke, there’s nothing to fix.” If, despite the board’s best efforts, an activist shows up in your stock, ignoring them will likely only make things worse. Until the recent sales, PL Capital had representatives on six boards, most of which didn’t initially want them there. “The [chairman] who says, ‘We would never put you on the board,’ that’s a trigger for me to demand a board seat,” Lashley says. “But if someone says, ‘Rich, I’d love to have you on the board,’ the minute I hear that, I think, ‘I don’t need to be there. They’re not entrenched. They’re thinking like a shareholder.’”

“It’s uncanny how often we decide to pass on pursuing activism based on the response we get,” he adds. **[BD]**

John R. Engen
is a writer and
contributor to
Bank Director.

Share this article

Sharing options are located in the right corner of the top navigation bar.

WHO THEY ARE



Swipe below to cycle through the activists targeting banks.



A growing number of activist hedge funds are setting their sights on the banking industry, including such large generalist funds as Trian Fund Management and Corvex Management, an \$11 billion fund that has recently taken small stakes in Bank of America Corp., Comerica and Citizens Financial Group. More familiar are these four investors that have been investing in banks for more than two decades:



Basswood Capital Management:

Co-founded and run by Matthew Lindenbaum and his brother Bennett, Basswood boasts more than \$2.5 billion in assets under management. The vast majority of the 22-year-old hedge fund's 169-plus equity holdings are bank stocks. It likes mid-cap regionals most of all, and isn't afraid to press for a sale: It was the driving force behind the 2015 sale of Astoria Financial.

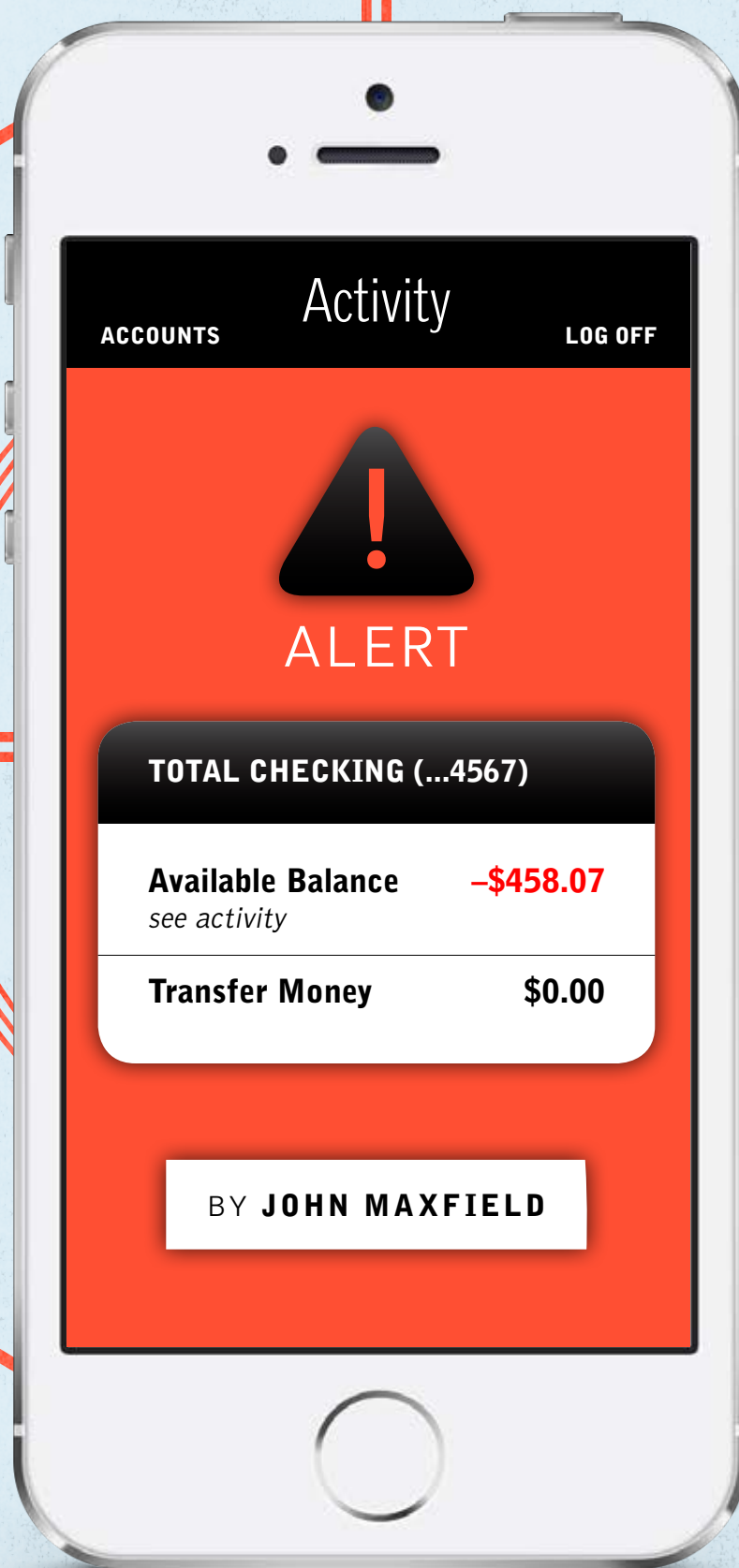
1

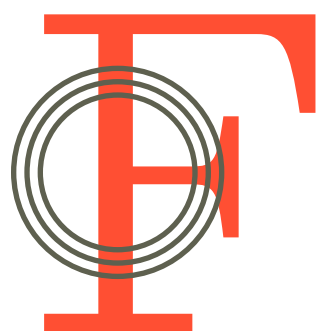


Targeting Fees

Regulators plan more changes to bank overdraft fees.

THE LEGAL ISSUE





Federal regulators have made it clear that they will soon implement rules that govern more strictly how banks assess overdraft fees. The expected move will be the first since regulators began requiring banks to get written authorization from customers to opt in to overdraft programs, starting in 2010.

The Consumer Financial Protection Agency (CFPB) announced in November that it is preparing to launch a rulemaking to increase consumer protections concerning overdrafts and checking accounts. The process, which is expected to kick off later this year, goes hand in hand with CFPB Director Richard Cordray's efforts to improve consumer access to financial products.

"Over the years, overdraft programs have become a significant source of industry revenues, and a significant reason why many consumers incur negative balances," said Cordray at a recent field hearing on checking account access. "Too many problems with overdrafts can cause people to give up on the banking system or force them out of it altogether."

To this end, the CFPB director sent a letter at the beginning of February to 25 of the nation's largest retail banks, suggesting that they offer lower-risk checking or prepaid accounts that eliminate the possibility that a customer can incur a negative balance. Cordray pointed in accompanying remarks to guidelines issued by the Federal Deposit Insurance Corp. (FDIC) for cost effective accounts that are safe and affordable for consumers, known as the FDIC Model Safe Accounts Template.


Cordray also cited the National Account Standards established by the Bank On movement, a consortium of partnerships between financial institutions and local communities. The standards build

on the FDIC's work by laying out more than two dozen account features designed to attract unbanked consumers. These include making overdraft fees all but impossible by offering checkless checking accounts that exclude overdraft services on debit card transactions.

Multiple banks had already heeded this call. In June 2014, for instance, Cleveland, Ohio-based KeyCorp's KeyBank launched its Hassle-Free Account, which allows customers to make deposits, track money, obtain cash and make payments without incurring overdrafts. A spokesperson for the bank said in an emailed statement that the lower-risk account "expands our ability to serve both the unbanked and those locked out of the banking system today."

Capital One Financial Corp. offers a similar product, known as 360 Checking, which permits overdrafts but instead of charging a punitive fee it assesses interest only on the amount of the overdraft. It also offers free transfers from a linked savings account to cover any overage. The McLean, Virginia-based bank didn't respond to a request for comment.

Beyond its efforts to encourage banks to offer lower-risk checking accounts, a CFPB spokesman made it clear that it will soon supplement rules that govern even standard checking accounts. The Bureau's latest rulemaking agenda highlights multiple "consumer protection concerns" related to overdrafts that it seems intent on remedying. These include the structure of overdraft and insuf-



"Too many problems with overdrafts can cause people to give up on the banking system or force them out of it altogether."

RICHARD CORDRAY | CFPB DIRECTOR



5 Best Practices

When Designing NQDC Plans



When designed properly your NonQualified Deferred Compensation Plan can have a positive impact by helping execs plan for retirement, retain and recruit top talent and provide long-term incentive and retention strategies. Utilize experts to help discover the best approach for your bank's success.

Compensation Advisors, a member of the Meyer-Chatfield Group, develops innovative new products like LINQS+. The most efficient SERP design available, LINQS+ decreases the cost of traditional SERPs up to 50% while providing an enhanced **lifetime benefit**.

Intimately familiar with core issues plaguing the banking industry, we deliver clear, insightful solutions that produce results.



JR Llewellyn
JR.Llewellyn@CompensationAdvisors.com
850-308-1468



James J. Calla
James.Call@MeyerChatfield.com
267-212-4384

ficient funds fees, the order in which banks post checking account transactions, and the way that consumers opt-in to overdraft coverage for debit card transactions.

The CFPB's concern about opt-in requirements manifested itself in an enforcement action that the Bureau brought last year against Regions Financial Corp., a \$126 billion asset bank based in Birmingham, Alabama. The CFPB fined Regions \$7.5 million and ordered it to refund roughly \$50 million in fees that it said had been assessed against customers who had not opted in for overdraft services. It was the first time that the CFPB has used its authority under Regulation E, which was revised in 2009 after Congress passed a law to require that customers opt in to overdraft protection.

The Bureau followed this up in October by notifying TCF Financial Corp. that it might take similar action against the \$21 billion asset Wayzata, Minnesota-based banking company. TCF responded to the CFPB's allegations in late November and believes that its overdraft opt-in practices comply with all applicable laws and regulations, said Mark Goldman, TCF's director of corporate communications, in an emailed statement.

The biggest problem with opt-ins, according to studies by the Pew Charitable Trusts, is that bank customers often don't understand how the process works. In a 2014 survey, Pew found that 52 percent of respondents who had overdrawn their checking accounts over the previous year did not recall opting into the service. Beyond this, "many consumers are confused about how the opt-in process works," says Susan Weinstock, Pew's director of consumer banking. "They think that opting in will allow them to avoid overdraft fees, when the opposite is in fact the case."

Pew has published a model disclosure box that banks can use to remedy this. It lays out general account information and dedi-

cates roughly a third of the one-page document to an explanation of overdraft services. Of the 45 large banks Pew evaluated in its 2015 report on overdraft practices, it found that 62 percent of them have adopted disclosure boxes that conform to its model.

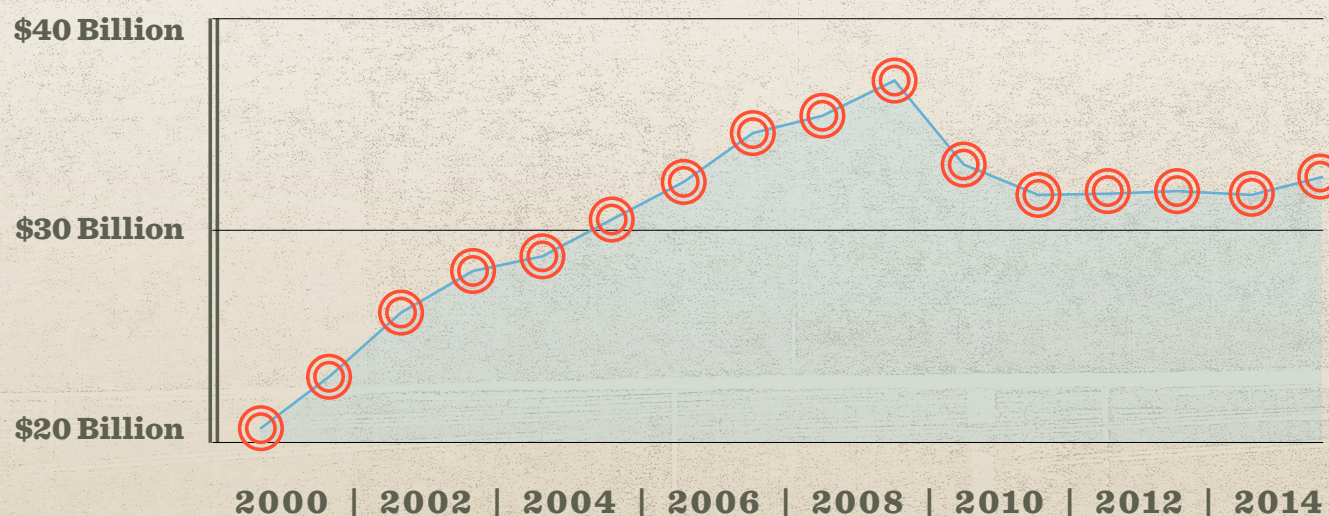
The impact of existing opt-in requirements on banks' bottom lines has been substantial. Since the Federal Reserve added the opt-in requirement to Regulation E in 2009—though the change didn't go into effect until the following year—only a third of consumers have agreed to the service, according to a 2015 study by Novantas Research. Bank consulting firm Moebs Services estimates that overdraft fees collected by both banks and credit unions dropped from a peak of \$37.1 billion in 2009 to \$31.6 billion in 2011.

“To be clear, the 14.8 percent drop in overdraft fees from 2009 to 2011 wasn't the result of the opt-in requirement alone,” says Michael Moebs, CEO of Moebs Services. “But it played a major role.”

In addition to disclosure, the CFPB has shown interest in regulating the design of overdraft services themselves. It is focused especially on reining in features that increase the number and extent of overdraft fees that customers incur, such as posting daily

Bank and Credit Union Overdraft Fees

After increasing consistently for a decade, industrywide overdraft fee revenue fell after Regulation E's “opt-in” requirement went into effect in 2010.



Source:
Moebs Services

checking account transactions from the largest to the smallest dollar amounts, as opposed to chronologically.

Many large depositories have already eliminated this practice, says David Pommerehn of the Consumer Bankers Association. They were incentivized to do so after paying hundreds of millions of dollars in legal fines and settlements stemming from the practice over the past decade. A federal district court judge in 2010, for example, issued a scathing indictment of the practice at Wells Fargo & Co., calling it a “draconian” bookkeeping device that “dramatically multiplied” the number of fees the bank could extract from a single mistake made by a customer. Wells Fargo declined to provide a comment for this article.

Weinstock believes that other features of bank overdraft policies are similarly likely to attract attention from the CFPB. These include reducing or eliminating extended overdraft fees (the fees banks sometimes charge when a customer hasn’t repaid the overdraft within a specified period of time), capping the number of overdraft fees assessed on a customer in any given year, and ensuring that the size of the fees are reasonable and proportional to the costs of the service. The Pew Research Trusts enunciates these and other best practices related to overdraft policies in its 2015 update to its Checks and Balances report.

There’s no question that overdraft services are important. “In many instances, overdraft services are the last refuge for consumers in need of immediate credit,” explained the CBA’s Pommerehn. However, it seems increasingly apparent that banks will soon no longer be permitted to design these services without taking into consideration a more holistic view of consumers’ best interests. **|BD|**

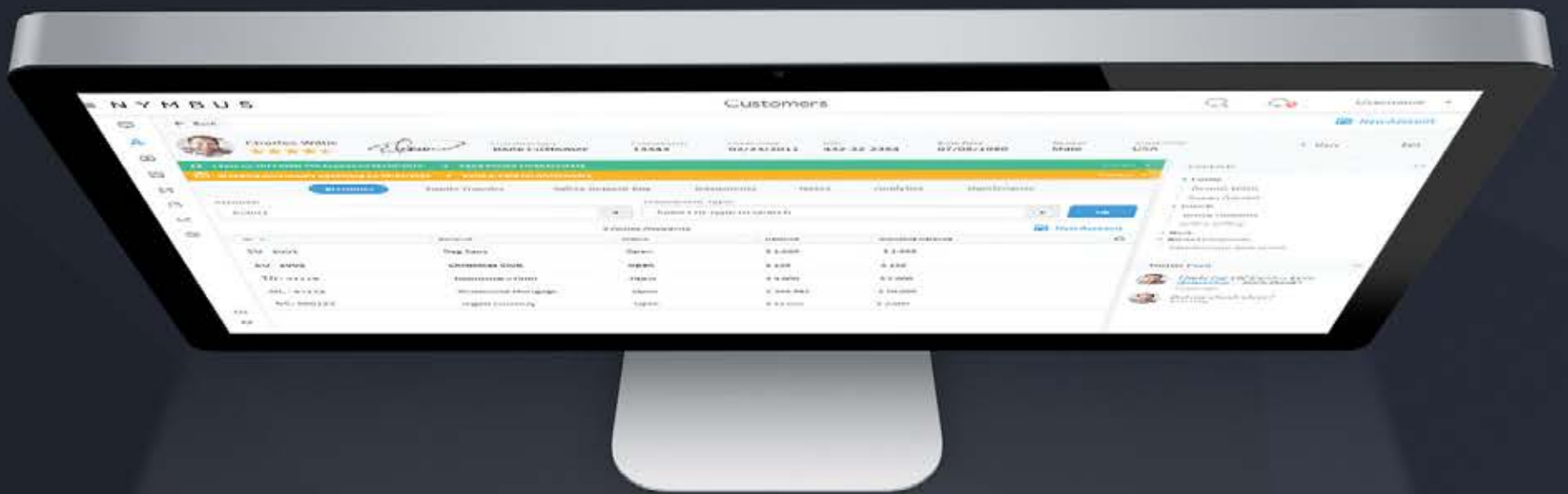
John Maxfield

is a writer and contributor to *Bank Director*.

Share this article



Sharing options are located in the right corner of the top navigation bar.



Increase Productivity



Reduce Operational Costs



Generate More Revenue



Increase Cyber-Security



Improve Compliance



Innovate Faster

NYMBUS

The Next Evolution of Core Processing

[illegible]

Here's what banks need to know about cybersecurity threats.

Cybersecurity seems like such a terrible threat, because it is mostly unknown. Bankers are confident that they can get their hands around the risk inherent in their commercial real estate portfolios. But how do they know what cyber criminals are doing and what risk they pose to the bank?

One of the newest regulatory developments is the publication of the FFIEC's cybersecurity assessment tool last year, which is designed to help

banks do exactly that. It's not a law and compliance is not mandatory per se, but when regulators say they are going to use the tool in exams, it quickly moves from a tool to an expectation, says Nathan Taylor, an attorney who specializes in cybersecurity at Morrison & Foerster LLP.

Boards are responsible for overseeing the organization's cybersecurity, and making sure staff is addressing the risk. To help with this endeavor, *Bank Director* digital magazine interviewed forensic investigators who work with banks to identify the gravest concerns.

For the purposes of this article, a cyberattack refers to a malicious attempt, whether successful or not, to invade an institution through its computers or servers. It may also include the instances where bank customers are tricked in some way to give up their online or mobile bank account usernames and passwords, and sometimes even security question responses. This obviously becomes a problem for the banks when they have unhappy customers demanding that funds be returned, not to mention going to the local media with their complaints.

Who Are the Attackers?

Attackers are coming from all over the globe, but they have been traced mostly to criminal organizations, many of them operating from Eastern Europe. They are extremely hard to find and prosecute. After a series of attacks on large organizations and banks from 2011 to 2013, including Bank of America, JPMorgan & Co, and the New York Stock Exchange, the U.S. Justice Department filed criminal charges earlier this year against seven Iranians they accused of acting in concert with the Iranian government to shut down the institutions' web sites. Needless to say, the Iranian government has not sent them to the U.S. to face prosecution.

More From Bank Director

+ Resources

For more resources, check out our [resource page](#).

+ Legal Responsibility

For more on the legal responsibilities of the bank, see our story on the [legal ramifications of a breach](#).

What Are Their Methods?

Malware, sometimes in combination with phishing, is still a huge threat for banks. Malware is malicious software downloaded on to your computer or smartphone, often without your knowledge. Phishing refers to the tactic of trying to obtain sensitive information, such as bank account log-in information or a social security number, usually with a seemingly legitimate email query.

“Phishing is still very prevalent,” says Ross Hogan, global head of fraud prevention at Kaspersky Lab. These methods could be used against bank employees, but more often, successful attacks are lodged against the bank’s customers, which the bank has less control over. “Users are vulnerable, unsophisticated and capable of being duped, and sometimes they’re just lazy,” says Hogan.

A common phishing method is to direct users to a fake web site that looks like a real web site or to an emailed attachment and simply ask for sensitive information such as online bank account log-in information. A customer might think this was a real inquiry from their bank. Newer types of malware distributed through infected apps on the smartphone will freeze the phone and demand the user type in sensitive information such as bank account information and passwords before unlocking the phone, says Ron Plesco, national lead of KPMG LLP’s cyber investigations.

Other types of malware will operate in the background and spy on the users’ behavior, storing information such as passwords and even the answers to security questions. “They can make sure the user has absolutely no knowledge this information was ever sent,” Plesco says.

```

10000110      11101000
11101000110100      0011001010000
0010111100101110      010011011101110
00110000101100100      11100111  00011001
1001100      1001000      011001  001011
000011      000000      111000  001011
011111      010111      010000  010000
001011      001011      0001011  0001011
010001      1101100001      00101111  00101111
1100010      000001110
00110001      10  1000011
000101010      111001  111001
11101100      1100011  1100011
101100110      1100011  1100011
11010001      001010  0100000
1001100      1001001  110100
0010111      1110110  00010000
0010100110111010001      10001100001011010
01011011100110010000      000111010001100
10101110010011010000      01101001011
11001110100010111100

```

23% of recipients of phishing emails open them.

```

10110      10110
010110      010110
1010110      1010110
010010110      010010110
11011100111      11011100111
10001000110011      10001000110011
1011001  111110      1011001  111110
101110  000010      101110  000010
101      001110      101      001110
010011      010011
000011      000011
000010      000010
110110      110110
110110      110110
101000      101000
010110      010110
000110      000110
000001      000001
000110      000110
100101      100101
010110      010110

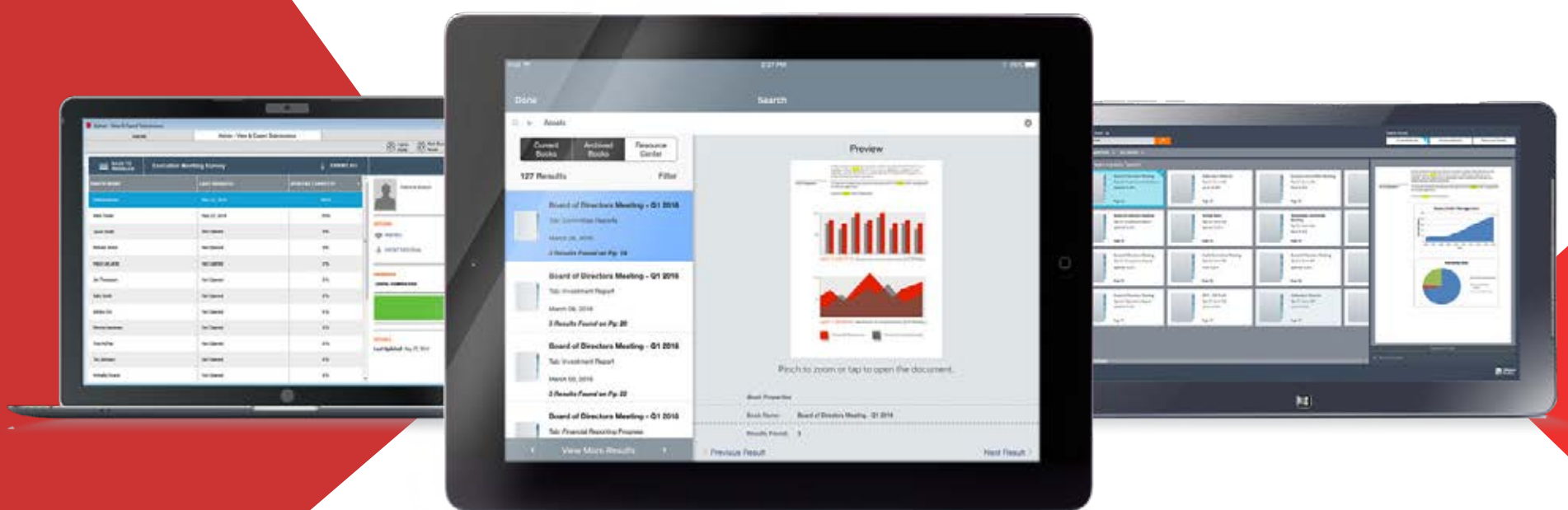
```

11% click through to attachments.

Source:
2015 Verizon Data Breach
Investigations Report

100,000+

of the world's top executives and directors agree on one thing.



They can rely on Diligent for their board communications.

Diligent Boards is the most trusted secure board communications and collaboration tool

- ▶ Simple, intuitive interface on iPad, Surface and PCs
- ▶ Advanced features like note sharing and e-signatures
- ▶ Best-in-class security and compliance
- ▶ 24/7 service from a real person

SCHEDULE A DEMO

- 1 877 434 5443
- info@diligent.com
- diligent.com



Diligent



Diligent is a trademark of Diligent Corporation, registered in the United States. All third-party trademarks are the property of their respective owners. ©2016 Diligent Corporation. All rights reserved

According to the Verizon 2015 Data Breach Investigations Report, 36 percent of confirmed data breaches at financial institutions involved “crimeware,” meaning malware that can capture sensitive log-in information, perhaps on a customer’s computer or phone.

Not all cyberattacks involve actual breaches. Roughly one-third of security incidents reported at financial institutions involved distributed denial of service (DDoS) attacks, according to the Verizon report, but investigators say most criminals target large and regional banks. DDoS attacks remotely exploit a weakness in a variety of computer systems and turn them into an army of computers, or a “botnet.” The computers’ owners may be unaware that their computers have been taken over and are attacking specific targets, such as banks and other companies, overwhelming their web sites so as to shut them down. Some criminals demand ransom payments to stop the attacks, or they steal data and encrypt it, threatening to destroy the company’s data or sell it unless a ransom is paid. Plesco and other investigators are seeing an increase in extortion tactics such as these.

What Are the Bank’s Vulnerabilities?

The financial industry is one of the top targets of cyber criminals in terms of numbers of incidents and data breaches, according to the Verizon report. Although several investigators said they believed the financial industry is generally better protected than many other industries, they felt that small banks didn’t have the resources to protect themselves as well as big banks.

In addition, several investigators said banks should be concerned about the vulnerabilities of increasingly popular mobile

Which Industries Have the Highest Number of Breaches?

Tap on the following to see the number of confirmed data breaches, by industry:

11101000 011001100 11101000
00100010000 1100100110110 00100010000
010010110110110 1101100110110 010010110110110
11100111 00011001 0111011 11001010 11100111 00011001
011001 001011 0001011 1011100 011001 001011
111000 001011 001111 1111100 111000 001011
010000 1000101 0111000 010000 0001011
0001011 0000110 101100 00011 110110001
1101100001 011100 00011 001011
0010111 101110 00011 0010111
000001110 0010110 001100 000001110
10 1000011 0101100 110111 10 1000011
111001 0100110 000011 111001
1100011 000101 000101 1100011
1110011 0101100 1010000 1110011
001010 0100000 1011100 1001101 001010 0100000
1011001 110100 1011011 011100 1001001 110100
11110110 00010000 0111010 11000010 11110110 00010000
1000110000101010 01000001101010 1000110000101010
00011010001100 1100100110100 00011010001100
01101001011 000001100 011010001011

+ Government:

+ Financial Services

+ Manufacturing

+ Accommodation

**325 breaches occurred in unknown industries.*

Source:

2015 Verizon Data Breach Investigations Report

devices. While most banks have strict controls over their employees' use of mobile devices to conduct the bank's business, the bank's customers are not so well protected. People assume their mobile devices are safer than their computers and they don't download security software or they only use free software, says Hogan. Also, people are simply less vigilant on their mobile devices, following weird links as they multi-task, says Hogan. "The mobile device is the adult pacifier," he says. Although attacks coming in from mobile devices are still relatively few in number of total reported breaches, most of them are targeted to Android phones and its operating system, says the Verizon report.

Threats from insiders are real and potentially more damaging, if less frequent, than attacks from outsiders. Banks should pay special attention to the super-users in their organization who have access to critical systems and data, monitoring their activities as well as suspicious behavior or unusual trends.

Vendors also are a huge risk for banks, as most banks give contractors access to sensitive customer data or critical IT systems. A Turkish man pleaded guilty earlier this year to a hacking scheme that manipulated a payment processor to raise the amounts on prepaid debit cards, then used teams of criminals holding the debit cards to extract \$55 million from ATMs in the U.S. in 2013. Plesco says banks need to do security audits, assess the security practices of their vendors, and scrutinize their contracts with these vendors to find out who is responsible in the event of a breach.

Taylor says his clients' greatest fear is about what hasn't happened yet: The bank losing access to its data or having its data destroyed by a bad actor. "What happens if they've wiped

Confirmed Breaches at Financial Services Companies:

36% involve
crimeware

14% involve payment
card skimmers

11% involve insiders

** Individual attacks could include multiple attributes.*

Source:
2015 Verizon Data Breach
Investigations Report

out your account database?” he says. The scary scenario, and the one you don’t hear much about, is the possibility of an attack so severe, your company can’t function for weeks or more.

To get a handle on the risk of such unknowns is nearly impossible. But one of the best ways to start the threat assessment process is to get good people working for your bank who can make assessments and recommendations. Nick Bennett, who leads intrusion investigations as a director for Mandiant, the consulting arm of FireEye, says he finds that many companies are too focused on buying software and not on hiring top-notch people to protect themselves from threats. Software, for example, can detect anomalies in transactions or online behavior, but if no one is watching the software’s red flags, the bank is in trouble. “Many organizations buy up technologies, but basically, if you don’t have the people in place who understand the technologies, they aren’t much use,” he says.



Check out the following resources for more information.

- + The FFIEC has published a guide to help financial institutions identify risks and determine cybersecurity preparedness called the [Cybersecurity Assessment Tool](#).
- + The [FFIEC’s IT Examination HandBook](#) has longed delineated the regulators’ expectations for the board, although it’s okay to give some of these responsibilities to an IT committee of the board.
- + Bank Director’s 2016 [Risk Practices Survey](#) reveals what banks are doing to protect themselves.
- + [Experian](#) has published a data breach response guide.
- + The law firm Hunton & Williams [explores the board’s role in cybersecurity](#).

THE BANK'S LEGAL OBLIGATIONS IN A CYBER ATTACK

Many security experts believe it's merely a matter of when—not if—a bank will experience a cyber attack. And if that occurs to your institution, you'll need a good attorney to guide you through the legal ramifications.

There are several.

For instance, privacy and notification laws are different in every state, and your bank will have to navigate that complex array of requirements in the event of a breach. Not all breaches have to be reported. Generally, if a breach compromises the personal identification information of one or more of you customers, they have to be notified, says Kevin Petrasic, an attorney at White & Case who specializes in regulation and cybersecurity. Attorneys general in some states also need to be notified. Think what would

“You don’t want counsel you don’t really know and have to rely on them for one of the most critical times in your existence.”

— **Kevin Petrasic**
attorney, White & Case

happen if you didn't report a breach and a customer was unable to take steps to protect his or her assets? The bank is potentially liable.

If you're a publicly traded company, you may also be obligated to report to investors any breach deemed material by your counsel.

If customers lost money in the breach, the Electronic Funds Transfer Act and Regulation E protect their assets and your bank will be on the hook. There is generally a \$50 limit to liability for customers who report a loss or electronic theft, as long as they report the theft within two business days after they find out about it. If they don't, the liability limit goes up to \$500. This applies to consumer accounts, but not necessarily commercial accounts, which are governed by the contracts you have with the customer. Some banks may delineate in those contracts what steps commercial customers should take to protect their accounts, such as dual control over any wire transfers, in an effort to protect the customer and the bank. The lack of a clear understanding of liability in the event of a breach has led to plenty of lawsuits and hard feelings between banks and their commercial customers.

To help protect the bank, it's important to have strong legal counsel on retainer in the event of a breach, says Petrasic. He suggests someone knowledgeable about regulations regarding cybersecurity and breach response. He also advises getting to know your attorney ahead of time, involving such counsel in your bank's planning for an incident, and even walking through some scenarios to test the plan. "You don't want counsel you don't really know and have to rely on them for one of the most critical times in your existence," he says. **[BD]**

Naomi Snyder
is editor for
Bank Director.

Share this article



Sharing options are located in the right corner of the top navigation bar.

Three Critical Challenges for Bank Audit Committees

By **Sal A. Inserra**

As the effects of the banking crisis continue to recede, regulatory agencies have shifted their focus. As asset quality concerns gradually diminish, regulators are scrutinizing corporate governance and risk management issues more closely.

In this environment, audit committees are being challenged to meet a higher standard regarding their understanding of their organization's risk profile and often must adapt their approach to reflect changing business priorities. Three areas of concern merit special attention as they present audit committees with significant challenges.

Challenge 1: Cybersecurity Risk

Cybersecurity is a paramount issue in financial institutions today, ranking as the number one concern of bank executives and board members in the annual Bank Director Risk Practices Survey for two years running. In the 2016 survey, 77 percent of the respondents said cybersecurity was their top concern, and more than half said preparing for cyber attacks is one of their biggest risk management challenges.

Those numbers are not surprising because banks are a natural target for hackers. But the challenge of managing cybersecurity risk is complicated by banks' natural reluctance to publicize breaches due to their legitimate fear of alerting other hackers to their vulnerabilities. Unfortunately, this justifiable secrecy makes it more difficult for other banks to learn from their peers' experiences and hinders banks' ability to recognize comparable weaknesses in their own systems and third-party relationships.

Another complicating factor is the makeup of the audit committee itself. Committee members very rarely have professional IT backgrounds, so they must rely on qualified third parties to provide insights into risks and mitigation strategies.



Three Critical Challenges for Bank Audit Committees

By **Sal A. Inserra**

members very rarely have professional IT backgrounds, so they must rely on qualified third parties to provide insights into risks and mitigation strategies.

Recent regulatory guidance can help overcome this challenge to some extent. Audit committee members should be thoroughly familiar with the Federal Financial Institutions Examination Council's two-part Cybersecurity Assessment Tool, which was issued in 2015 to help institutions identify their risk exposure and determine if their risk management programs are appropriately aligned. The audit committee should make sure management completes this assessment and integrates its principles into the overall risk management effort.

In addition, the Office of the Comptroller of the Currency (OCC) regularly issues joint statements with other bank regulatory bodies on specific cybersecurity concerns such as new malware developments, extortion attempts, and other current trends. Committee members should stay abreast of the most recent OCC statements on the agency's website and confirm that management is following the specific preventive steps listed in those statements.

Challenge 2: Reallocating Audit Resources

In the current industry environment of shrinking margins and growing cost pressures, audit committees often must address increasing regulatory compliance demands and growing cybersecurity risk while struggling with resource constraints. Fortunately, there often are unrecognized opportunities to control risk management costs by reallocating resources to reflect changing business models.

For example, as customer habits and access methods change, some financial institutions are reassessing whether it is cost-effective to continue applying the same level of risk mitigation activity at the branch level. Steps such as lengthening the intervals between traditional branch audits and reassigning certain risk control respon-



Three Critical Challenges for Bank Audit Committees

By **Sal A. Inserra**

of risk mitigation activity at the branch level. Steps such as lengthening the intervals between traditional branch audits and reassigning certain risk control responsibilities to operational managers make it possible to reallocate some internal audit resources to new, more pressing areas of risk. Audit committee members should be alert to such opportunities to reassess and fine-tune the audit approach to reflect today's business reality.

Challenge 3: Adapting to New Strategies

Shrinking margins also are leading banks to look for opportunities to diversify their revenue strategies. But every new revenue stream requires new operational and support functions and opens up new categories of risk that must be assessed, controlled, and managed. One of the important responsibilities of the audit committee is to actively assess how a new business line will affect the institution's risk parameters and to determine how those parameters can be addressed effectively and efficiently.

New revenue streams and changing business strategies are nothing new, of course. Historically, bank directors always have been challenged to adapt to shifts in economic and business priorities. In today's environment, however, with greater regulatory emphasis on the management of risk, the challenges to audit committees are intensified. An effective response to these challenges can have a direct, significant and positive effect on an institution's long-term success.



Sal Inserra is a CPA and partner with Crowe Horwath LLP and can be reached at +1 404 442 1608 or sal.inserra@crowehorwath.com.





THE LEGAL ISSUE

BY ADAM O'DANIEL

PENALTY FINES GET LARGER AGAINST DIRECTORS

The average civil money penalty increased 15 percent in 2015.

Two trends appear to be developing in the world of civil money penalties levied against bank directors, creating a mixed bag for board members. Since 2014, the number of bank directors ordered to pay civil money penalties by the Federal Deposit Insurance Corp. (FDIC) has dropped dramatically, but the average

penalty has increased by more than \$10,000, or about 15 percent.

Regulators can assign civil money penalties against banks, bank directors and bank officers for a variety of reasons, including negligence, mismanagement, improper use of funds and a host of other improprieties. As the financial crisis reaches the decade mark, fewer directors and officers are getting hit with fines, but the dollar amounts of those fines don't seem to be falling.

In 2012, 48 individual directors were slapped with fines. The number dipped to 39 directors in 2013 and crept back up to 44 directors in 2014. The average penalty in those years? About \$67,000.

Then, last year, the numbers made a noticeable shift. Only 27 individual directors faced orders from the FDIC to pay civil money penalties for various misbehaviors on the job, a 38 percent decline.

However, the average dollar amount for those penalties jumped 15 percent to \$77,759.

"There definitely seems to be a shift to higher severity, but lower frequency, when it comes to civil money penalties," says Dennis Gustafson, a principal at AHT Insurance who provides directors and officers' liability insurance. "Is that intentional? It's hard to say."

An FDIC spokesman did not respond to requests for comment.

Civil money penalties also are assessed against directors at nationally chartered banks by the Office of the Comptroller of the Currency. However, these fines have been much smaller and fewer in number than the more active FDIC. In 2015, the OCC handed out 21 civil money penalties with an average fine of \$17,091, increasing from an average of \$6,948 in 2014.

Insurance: To Buy or Not to Buy

The issue is of particular interest to directors because banks normally buy directors and officers (D&O) insurance for the board



CIVIL MONEY PENALTIES

+ FDIC

+ OCC

Tap FDIC or OCC to view the penalty statistics from each.

and management to insure against liabilities such as shareholder lawsuits. But banking regulations prohibit financial institutions from insuring or indemnifying individual directors in the event of a civil money penalty.

“That rule has been in place for years,” says Scott Simmonds, an insurance consultant for financial institutions. “However, it has been brought back to the forefront in recent years with new guidance and heightened awareness.”

“The FDIC tends to send a warning shot first.”

SCOTT SIMMONDS,
INSURANCE
CONSULTANT

In October 2013, the FDIC released an advisory statement to all members, alerting boards of directors that civil money penalties cannot be covered by their bank-paid D&O insurance. Further, the FDIC expressed its interpretation of the rule to also mean banks can’t pay the premiums on separate civil money penalty (CMP) insurance or pay the penalties on the director’s behalf. The board members themselves are responsible for any assessed CMPs.

When the guidance was first released, the news sparked sudden interest from directors’ associations and banking industry media. Gustafson says he received phone calls from at least one-third of his clients asking how they should properly insure themselves in light of the rule.

Insurance companies, including AmTrust Financial Services, began underwriting policies sold to individual directors. Such policies were believed to be within FDIC guidelines because the premi-

The best way to avoid a civil money penalty: “Just do the right things as a director everyday.”

HARRY DAVIS,
BOARD MEMBER,
YADKIN BANK

ums had to be paid by the individual directors, not the institutions.

However, over the past year or so, Gustafson says interest in the policies has cooled. He’s still offering the product—premiums average about \$830 for \$50,000 of coverage—but he’s not sure it will ever be widely purchased.

“There just isn’t a lot of fear out there right now...It may remain a niche product,” he says. “A couple years ago, more banks were under regulatory orders. Those bankers were a little more concerned.”

Ironically, Gustafson says he analyzed banks hit with civil money penalties in the past year and found 71 percent were stable lenders, not insolvent institutions. He also says the higher average penalty may cause some directors to reconsider. “Just because your bank is healthy doesn’t preclude you [from a CMP],” he says. “It’s still a new product, so we will see where it all goes.”

Best Insurance: A Clean Bank

Harry Davis, a board member at Raleigh, North Carolina-based Yadkin Bank, says regulatory oversight and civil money penalties are on the radar for most directors. Davis, who also teaches banking and economics at Appalachian State University, says conversations about D&O insurance are standard practice, but his colleagues prefer to focus on doing their jobs well more than how well they’re insured.

“The best approach is to operate with heightened scrutiny, stay educated of all the changing regulations and then focus on leading and overseeing a really well-run bank,” he says. “That’s the best way to avoid a civil money penalty. Just do the right things as a director everyday.”

Simmonds, the Gulfport, Mississippi-based bank insurance consultant, says he often focuses on the odds when evaluating civil money penalty insurance for individual directors. He points out there are thousands of independent directors across the country, and fewer than 100 annually have been ordered to pay civil money penalties the last five years.

“That’s just a really small percentage,” he says.

He works with about 400 clients, mostly banks with less than \$5 billion in assets, and most of those directors choose not to purchase additional insurance. He said the bigger issue for most boardrooms when it comes to insurance is the risk involved in cybersecurity.

“The FDIC tends to send a warning shot first. If you heed the warning, there’s no penalty. It’s directors who ignore the warning shots that end up getting shot between the eyes,” he says. “On this issue, to me, the best insurance is usually just running a really clean bank.” **|BD|**

Adam O’Daniel
is a writer and
contributor to
Bank Director.

Share this article



Sharing options are located in the right corner of the top navigation bar.



A BOARDROOM CONVERSATION

Unlocking Shareholder Value

James “Jim” Chiafullo is a director at F.N.B. Corp., a \$20 billion asset bank holding company for First National Bank in Pittsburgh, Pennsylvania. In his day job, he’s a partner with the law firm Cohen & Grigsby, and chairman of the commercial finance group. He is passionate about corporate governance, and explains why he cares about concepts such as duty of care and duty of loyalty.



James Chiafullo
is a director at
F.N.B. Corp.

You really care about corporate governance. Why?

I was a summer associate [and later attorney] at the Gulf Oil Co. in Pittsburgh [in the 1980s]. It was a wonderful company that was generous with the communities in which it operated. [However,] the board of directors at Gulf lost sight that the shareholders owned the company and shareholder value was an important part of their obligation. The company’s stock traded between \$28 and \$35 per share. When you looked at their balance sheet, you saw there was cash on hand and proven reserves of oil and gas of about \$100 per share. By not unlocking that value, it made them very vulnerable to activists. At that time [in 1979], it was Mesa Petroleum and T. Boone Pickens. [Pickens] suggested a royalty trust that really worked as a way to break up the company and release that value. It was not good for anybody, really. The shareholders got some benefit, but they would have been better off if a path of releasing that shareholder value was taken by the directors. That’s what was missed. The [directors] were all very smart people. They lost their way. They missed how



A BOARDROOM CONVERSATION

Unlocking Shareholder Value

taken by the directors. That's what was missed. The [directors] were all very smart people. They lost their way. They missed how important it was to return shareholder value. It's a really important part of what I'm thinking when I'm sitting in the boardroom. I was lucky enough to be a first hand observer of all this. I was a young lawyer.



James Chiafullo
is a director at
F.N.B. Corp.

How does that fit into the duty of care and the duty of loyalty?

You have to be prepared at all time for decisions and meetings. You cannot feel like you have a right to be in that boardroom. You can't be entrenched. You have to make the decisions that are in the best interest of the shareholders, not you, but the shareholders.

What skills can a lawyer bring to a bank board?

He can bring corporate governance skills and risk analysis. That's a very important part of bank boards presently. Risk is one of the most important committees.

One CEO told me that it's important to listen to his lawyers' advice but not necessarily take it because lawyers are too focused on avoiding risk, and sometimes you just need to make decisions based on what's best for the company. Do you think that's true?

I could not agree with him more. A lawyer is a tool like any other tool in a businessman's toolbox. You can't abdicate your



A BOARDROOM CONVERSATION

Unlocking Shareholder Value

other tool in a businessman's toolbox. You can't abdicate your responsibility to lawyers. The whole idea of being a director is to assess risk and make decisions that lead to reasonable rewards. I should never be giving legal advice when I'm on the board. That's not my role. We have excellent general counsel at F.N.B. Corp. He comes in with the legal perspective.



James Chiafullo
is a director at
F.N.B. Corp.

You have a pretty extensive document on your web site called “directors’ duties and responsibilities.” What struck me was that everything was very clearly spelled out in terms of what to do if you have a potential conflict of interest, and even defined insider trading and said no member of your family can sell stock within 48 hours of significant news about the company going public. Is that level of detail needed?

In that arena, you want to err on the side of conservatism, especially on insider trading. There is nothing gained by playing that fast and loose.



IS THE BANKING INDUSTRY TOO SAFE TO BE SOUND?

Bank Director speaks with San Francisco-based Bank of the West Chairman J. Michael Shepherd, who has a background as general counsel and former CEO of the \$76 billion asset institution.



How often does your board review technology issues, including cybersecurity?

BankDirector. Strong Board. Strong Bank.

SAVE THE DATE

UPCOMING EVENT

June 14-15, 2016

Chicago | *Swissôtel*

BANK AUDIT & RISK COMMITTEES CONFERENCE

Insight On Oversight

Key Issues Covered Include:

- + Data Security
- + Fraud Prevention
- + Crisis Management
- + Emerging Technology
- + Effective Internal Controls

“Overall an excellent conference. Rich content, well prepared speakers and relevant, current information.”

—Past Bank Audit & Risk Committees
Conference Attendee

Register Now



Tap to
Register Now!



BankDirector. Strong Board. Strong Bank.

EXPLORE + SHARE



SWIPE UP

Scroll through
BankDirector.com
and tap an article
to read the full
version.

BankDirector.com

An Online Information Resource
On All Things Bank Board-Related

View these articles and more at **BankDirector.com**

BankDirector®

Digital Magazine

THE LEGAL ISSUE

President & CEO

Al Dominick

Chief Operating Officer

Mika Moser

Editor

Naomi Snyder

Publisher

Kelsey Weaver

Client Relations Manager

Laura Proffitt

Art Direction and Design

Robertson Design

Marketing Manager

Robert Phelps

Circulation Associate

Claire Kennedy

Controller

Ryan McDonald

Bank Director Senior Leadership Team

Board of Directors:

Chairman Joan Susie, Al Dominick,
Mika Moser, Kelsey Weaver
*and Founder and Chairman of
the Executive Committee*
Bill King

Editor in Chief

Jack Milligan

Vice President, Conferences and Chief Project Officer

Laura Schield

Chief Brand Officer

Michelle King

Bank Director is published eight times per year digitally and four times per year in print by DirectorCorps Inc., 201 Summit View Dr., Suite 250, Brentwood, TN 37027. The entire contents of *Bank Director* are copyright ©2015 and may not be reproduced in any manner without written permission. All rights are reserved.

Contact us

To get on the mailing list to be notified about new digital issues or subscribe to the print magazine, contact:

✉ **Circulation** | circulation@bankdirector.com

For editorial inquiries, contact:

✉ **Naomi Snyder** | nsnyder@bankdirector.com

For advertising opportunities, contact:

✉ **Kelsey Weaver** | kweaver@bankdirector.com



Like us on
Facebook



Follow
Bank Director
on LinkedIn



Follow
@BankDirector
on Twitter



Watch educational
videos on
Bank Director's
YouTube Channel