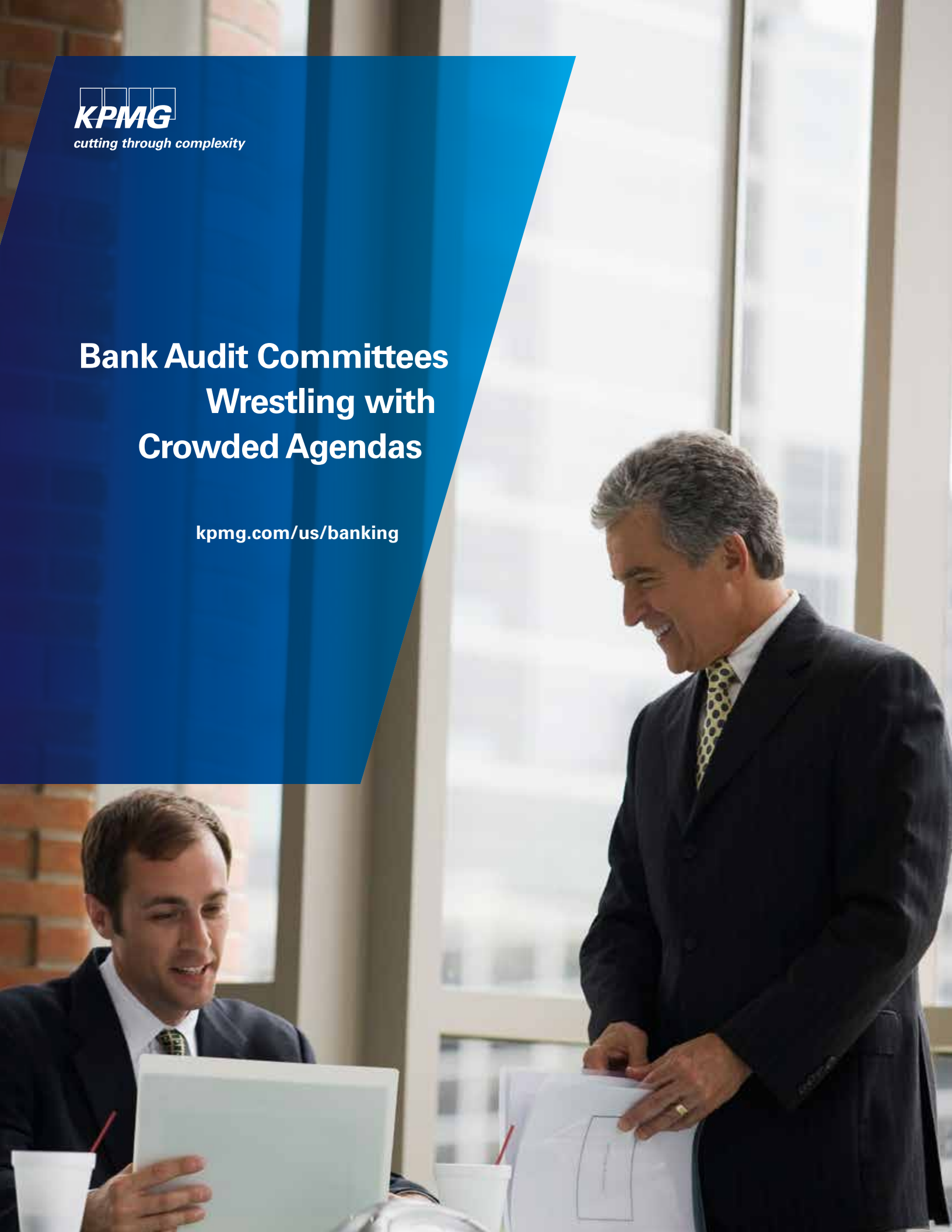
KPMG

cutting through complexity

Bank Audit Committees Wrestling with Crowded Agendas

kpmg.com/us/banking



Although financial reporting and internal control risk continue to share top agenda spots with regulatory compliance issues, bank audit committee chairs at a September 19, NYSE Governance Services, Corporate Board Member peer forum cosponsored by KPMG LLP (KPMG) said the focus of their attention continues to broaden considerably in the post-Great Recession era.

Among the other key issues vying for their attention, audit committee chairs at the forum inside the New York Stock Exchange said technology concerns – particularly those involving cyber security risks, growth through mobile banking applications, and upgrading information technology (IT) platforms – are gaining a high profile.

Further, they said, they are placing more focus on risk management, the effectiveness of internal audit, and proactive engagement with regulators in this prolonged period of tight net-interest margins, slow top-line growth, and an increasingly fickle customer base.

Given the array of traditional and emerging demands, the peer forum attendees expressed concerns about oversight overload – and their ability to keep pace with the speed of change that is shaping the banking industry. From the basic issue of having adequate time to focus on their crowded agendas, to the broader concern about having the requisite expertise to oversee management's plans to employ new technologies to connect with customers, the audit committee chairs aired numerous worries about the ability to maintain a high-level of effectiveness moving forward.

Fast Facts

The Banking Industry Audit Committee Peer Forum

Sponsored by:

- KPMG's Banking and Capital Markets practice
- NYSE Governance Services, Corporate Board Member
- Day Pitney LLP

Attendees:

- Audit committee chairs and members; risk committee members from 30 large and smaller banks from across the United States.

Attribution of Comments:

- In order to encourage candid conversation while being able to create an accurate report, participants were assured that their names would not be used in this publication.

Peer Forum Agenda

The day-long event, which attracted audit committee chairs from 30 banks ranging in size from less than $1 billion to almost $200 billion in assets, allowed participants to share their ideas, comments, warnings, and frustrations. Some observations were met with general agreement; others were debated aggressively. The session highlighted an array of topics, including:

- Financial reporting and internal control risk
- Regulatory compliance and reporting
- Enterprise risk management
- Capital and liquidity demands
- Revenue-replacement strategies
- Cost containment
- Building "best-in-class" audit committees
- Increased focus on the role of internal audit and its reporting structure
- Outsourcing of the internal audit function
- Third-party/vendor risk
- The separation of the risk and audit committees, and their specific roles
- Establishment of a technology committee of the board
- Restructuring of the balance sheet.

In terms of the current issues driving their agendas, there was a wide variety of responses:

"Our top priority is growth. The focus is on quality assets."

"We're actively looking at other businesses to complement our core – to bolster our non-interest income."

"Profitability and higher capital levels, those are the top items."

"With all of the new complexity these days, we need to better understand how we measure success."

"As a smaller bank, our biggest fear is surviving. The cost of compliance is enormous – and we have outsourced the work. Honestly, it's our biggest worry."

"We have outsourced so much of our operation that vendor management is right at the top for us. At one point this year, until we changed things, we had more outside vendors than employees."

"At our bank, we are highly concentrated – a one-trick pony in the mortgage market. So, we are trying to expand into the commercial market. We think the best way to do that is through organic growth. But, we need to be able to measure our progress very accurately."

"At our bank our main objective is customer service, customer attraction, and customer retention. At the moment, we have 32 incentive programs running – movie passes, cash gift cards, discounts, pens … ''

Following is a synopsis of three major themes – regulation, cyber security, and cost optimization. Participants agreed to allow their comments to be used in this report, provided that neither they nor organization would be identified by name.

Regulation

The uncertainty and scope of regulatory demands continues to be a central focus of the work on the agenda of the bank audit committee chairs in attendance. Still, some audit committee chairs noted that their organizations have accepted the idea that the added amount of time and effort required has become almost routine. A chair from a midsize bank noted that although "regulatory demands are maddening, and they can be overwhelming at times, I get the sense that things have … fallen into a predictable pattern ... It isn't such a mystery anymore."

Still, banks remain frustrated, they said, with having to spend so much time on the array of regulatory issues at the expense of such key issues as growth, cost containment, IT platform enhancement, improving customer relationships, and improving capabilities around data analysis.

In the discussion about regulation, there was considerable debate about the idea of having regulators regularly attend audit committee meetings.

A veteran audit committee chairman at a major regional bank initiated a lively give-and-take when he revealed that his committee has a federal regulator at every audit committee meeting. "The later they come in, the harder they come down on you," he responded when an audit committee chair from a midsize bank argued that a regulator in attendance at every meeting would "stifle open discussion" and eventually lead to "ineffective meetings." In response, the regional bank director said his board has learned that "our regulators are interested in seeing that management and the board are actively interacting on compliance and reporting issues." With regulators attending, he said, it not only demonstrates the committee's willingness to be open with regulators, it also adds incentives for the organization to follow through on compliance matters.

> *Among the notable comments on regulation compliance and reporting:*
>
> *"The CFPB (Consumer Financial Protection Board) is asking us for so much more detail than our other regulators. We are spending so much more time there (CFPB) than we had anticipated."*
>
> *"The main worry is about the focus on 'abusive transactions.' Compliance there will be a major focus."*
>
> *"My advice to anyone in the business now is to never get to the point where you think you know all there is know (about regulation). That can be dangerous."*
>
> *"One of our key issues right now is reviewing the ability of our vendors to stay current with regulations. It's a worry because our regulator is asking about that a lot lately. If your vendor makes a mistake, you can't send a letter to your customers or to your regulator that says, 'It wasn't our fault; it was our vendor.' It really is your fault."*

Cyber Security

In addition to revealing myriad cyber security vulnerabilities, the discussions uncovered a need for audit committees and management to collaboratively escalate efforts about threat awareness, timely discovery of incidents, risk assessments of vendors, and closer coordination with regulators about how cyber security risks are being identified and managed.

During the event's keynote panel discussion, a former chief information officer from a major global bank cited more than 200,000 cyber attacks a day directed against banks from rogue nation states, organized crime syndicates, and "hacktivists." Thus, board members agreed that significant work remains. Specifically, audit committee members heard that continued attacks without appropriate defense and response will damage their bank's brand and reputation, and can potentially result in significant financial loss.

A Federal Bureau of Investigation (FBI) cyber crime specialist joined the CIO in encouraging the audit and risk committee chairs to face up to what they called one of the fastest-growing areas of crime directed at banks. Cyber criminals, they warned, are exploiting the speed, convenience, and anonymity that modern technologies offer to invade bank information technology (IT) systems. The financial impact, coupled with the reputation damage, they said, could be devastating.

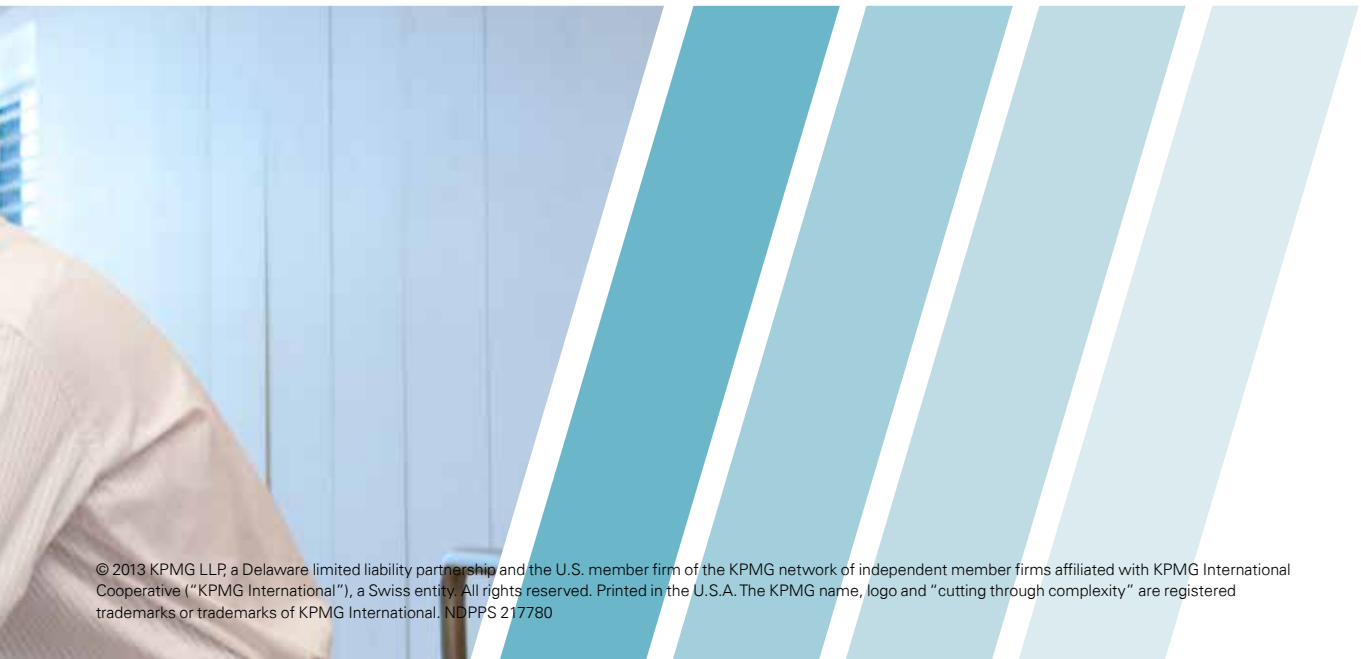
"You're not dealing with an IT department problem; it's an organization-wide problem," with a scope that the industry only now is beginning to appreciate, the FBI warned. "Boards still are not discussing this major problem in enough depth," the former CIO said. "It's getting better, but you're still not comfortable enough to challenge management on these issues."

When a board member from a large regional bank suggested, "We don't know what we don't know," heads in the room bobbed in agreement.

In 65 percent of the bank cyber attack cases handled by the FBI last year, the federal agency actually alerted the bank security teams because the bank did not know it had been breached, the FBI agent told the audience. "Much of the focus is on building defenses, which, unfortunately, are easily overcome," the FBI agent said. Many – and maybe most – banks, he added, "do not recognize that a breach has occurred … and they don't know what information has actually left the organization," as a result of the attack.

The FBI and the former bank CIO strongly suggested that audit committee members immediately meet with their bank management team and get an understanding of how their organization is monitoring cyber security effectiveness.

Very often the focus of denial of service attacks – typically a massive in-flow of e-mails or information requests to the banks computer system – is a diversion tactic. The true aim of the attack is to penetrate the information system to steal valuable information.



The advice offered was direct: Find out whether the bank's most valuable information is segregated – on a stand-alone, internal computer system – that cannot be accessed using the Internet – even by employees. Your main focus has to be to protect the crown jewels," the former bank CIO said. "Keep the crown jewels away from your Web-facing site."

According to the former bank CIO, most banks – and other organizations that are cyber crime targets – share one very vulnerable characteristic: Unwitting employees. In addition to denial of service attacks, cyber criminals target employees using "social engineering," a kind of con-game that manipulates employees into releasing valuable business information. Criminals may use former bank employees who supply telephone access information to contact bank employees, who then unwittingly allow the criminal into the bank's internal computer portals.

Another effective ruse is the use of thumb drives loaded with malware that are left in bank parking lots or in bank offices. "We've tested this by intentionally leaving thumb drives on floors, and then monitor who in the bank picks them up and plugs them in their bank computers," the former CIO said. "You'd be surprised how often people simply pick them up and plug them in." He added that, "security is not a one-and-done thing ... It is not a deliverable. It is a process. It unfortunately has become a cost of doing business that today is unavoidable"

Revenue Growth and Cost Optimization

Although aggregate industry net income has increased steadily since 2010, industry revenue remains weak – reflecting narrow margins and modest loan growth, among other factors. The industry's bottom line continues to benefit from reductions in loan-loss reserves, while a major cause of revenue weakness is ongoing tightness in net interest margin, which stands at its lowest level since the fourth quarter of 2006[1].

Those indicators are keeping pressure on banks to build the top line, which – in turn – is raising the stakes for audit committees to understand the risks management is taking on in its goal to grow.

Forum participants identified a number of initiatives in the name of growth. They would like to make more loans, but their loan standards have risen considerably and their qualification process is taking much more time than in the recent past, which is hampering loan revenue.

For some, the issue of growth and cost optimization has led to a fundamental reexamination of their business model.

"We are aggressively looking at other geographies."

"Our expansion plans include getting into the health care market, agriculture, and the energy industry. They're all new for us."

"We're moving into leasing … we bought a national company that focuses on leasing to small businesses."

"We've hired some very experienced people to help us expand into agricultural lending."

"One of the greatest challenges we see is getting Generation X involved in buying homes ... But, we also worry that the residential mortgage market is very competitive right now, and probably terribly underpriced."

"The idea of reinventing how we use branches intrigues us, but, like everyone else, it's an elusive thing. (Branches) are necessary for customer connection and brand purposes, but it isn't easy to measure the return on the investment."

"In some ways, we've created a demoralizing atmosphere with what we call a 'continuous improvement culture,' which really is aimed at driving down costs ... That almost always means a focus on staff reduction. That needs to be offset with growth, which is very hard right now with the increase in staff to deal with compliance."

[1] 2013 stlouisfed.org

At KPMG, our Banking & Capital Markets professionals embrace the opportunity to help industry executives better understand and manage the array of complex issues that are shaping banking. Our thought leadership, participation in industry events, and facilitation of knowledge-sharing events are offered as a means of encouraging dialogue and engagement. We welcome your participation in the debate, and ask that you reach out to any of these KPMG professionals:

Brian Stephens
National Sector Leader, Banking & Capital Markets
312-665-2154
bbstephens@kpmg.com

Judd Caplain
National Advisory Industry Leader, Banking & Diversified Financials
212-872-6802
jcaplain@kpmg.com

John Depman
National Regional & Community Banking Leader, Banking & Capital Markets
267-256-1631
jdepman@kpmg.com

Mark Price
National Tax Industry Leader, Banking & Capital Markets
202-533-4364
mhprice@kpmg.com

Dave Reavy
National Professional Practice Leader, Banking & Capital Markets
212-909-5496
dreavy@kpmg.com

Peter Torrente
National Audit Industry Leader, Banking & Capital Markets
212-872-5815
ptorrente@kpmg.com

kpmg.com/us/banking