FDIC Community Banking Conference: *Strategies for Long-Term Success*

Transcript

Panel 3: Managing Technology Challenges

Moderator: Mark S. Moylan
Deputy Director, Division of Risk Management Supervision
Federal Deposit Insurance Corporation

Panelists: Shaza L. Andersen
Chief Executive Officer and Founder
WashingtonFirst Bank, Reston, Virginia

Neil D. McCurry Jr.
President and Chief Executive Officer
Sabal Palm Bank, Sarasota, Florida

Michael Seifert
Vice President, Enterprise Risk and Resilience
Fiserv, Brookfield, Wisconsin

Robert A. Steen
Chairman of the Board and Chief Executive Officer
Bridge Community Bank, Mount Vernon, Iowa

MR. MOYLAN: My name is Mark Moylan. I'm the Deputy Director of Operational Risk here at the FDIC. I'm actually responsible for IT examination and policy programs as well as cyber security and some cyber infrastructure initiatives. I certainly want to welcome our panel.

Immediately to my left is Ms. Shaza Andersen. She is Chief Executive Officer and founder of WashingtonFirst Bank here in Reston, Virginia. Next we have Neil McCurry. He is President and Chief Executive Officer of Sabal Palm Bank in Sarasota, Florida. And next we have Robert Steen. He's Chairman of the Board and Chief Executive Officer of Bridge Community Bank from my old region in Mount Vernon, Iowa. And lastly is Michael Seifert. He is Vice President of Enterprise Risk and Resilience for Fiserv. So we have a TSP [technology service provider] on this panel.

This is certainly going to be interesting. I do want to kind of frame up what we're going to do. I've promised all my panelists we are not going to have a technical discussion. I promise you we are not going to talk about firewall configuration or the digital footprint of Thor malware. For those of you who understand and may have seen, the FDIC did a cyber awareness outreach

program in the last half of last year in all of our various regional offices, and one of our themes was taking cyber security from the server room to the board room. And, really, this discussion today is, again, carrying on the innovation and opportunities that technologies bring to the community bank but also how to manage it and how it factors into that. We are not going to be technical. This is really a conversation at the level that I'm most comfortable with, and that is at the executive manager or board level. What we're going to do to kick it off, I'm going to ask each of our panelists to again, introduce themselves and tell you all a little bit about their bank but, more importantly, what their IT profile may be.

So, with that, Shaza.

MS. ANDERSEN: Thank you, Mark. I'm really pleased to be here representing WashingtonFirst Bank from Reston, Virginia. We're a $1.8 billion bank with 19 branches in Virginia, Maryland, and D.C. And being here for this IT panel, it's an area that we're all interested in. When I started in banking, I still remember on Fridays when the line would be out the door with everybody coming in to make their deposits and get their cash for the week. Well, those days are gone. Nobody comes into the bank anymore. But, having said that, I am still a big believer in brick and mortar, because people want to know where their money is. They want to be able to see it. They want to know that if the systems go down, they could walk into a branch and be able to get their cash.

We offer all the technology that you can think of at our bank at WashingtonFirst. We have online banking, mobile banking, remote deposit capture, ACH [Automated Clearing House] wire transfer, being able to take your deposit via your iPhone and your mobile device. And that really has helped the community banks like us be able to compete by not having a location around every corner.

So, with that, again, I thank you, and I look forward to the conversation.

MR. McCURRY: Thank you. I'm Neil McCurry with Sabal Palm Bank in Sarasota. I'm going to state that when I was asked to be on this panel, I thought we were going to have to talk about technology things. So I brought my IT guy sitting in the front row over here. So if you want to know about our firewall, you can ask me. We have a complicated code system where he'll give me the answers, and I'll repeat them to you.

Sabal Palm Bank is a ten-year-old bank and has really had two segments to it. It was founded in Florida in 2006. With the benefit of hindsight, it was one of the worst times to start a bank in Florida with the crisis going on. I wasn't involved in the inception of the bank, but four years ago the bank had some capital challenges and I worked with the board of directors to recapitalize the bank and came in as the CEO and built up a management team.

So the first six years or so, the bank was really playing defense the whole time and wasn't focused on anything really much more than surviving. And then, when we got there, we really tried to change the profile to play more offense. We had more capital and had addressed some

of the issues. I think technology is great. To be clear, we are not an Internet-based bank, but we use technology to complement our business. We've been an adopter of a lot of technology over the last three years, and, you know, it certainly comes with trials and tribulations that you have to work through. But I think it's something that I'm very excited about, and I think it's a great time to be in community banking. I love it as much as I ever have, and I think it's an exciting time.

MR. STEEN: Thank you. I'm Bob Steen. I'm one of the under-$100-million banks that we're all worried about, and you should be worried. Our charter goes back to 1903. I've been there a long time, not that long. You know, we were chartered ten years before the Fed Act and almost 30 years before the FDIC Act. So, I just offer up to the FDIC and the Fed, as you continue to mature, if there's anything we can do for you, just ask.

My perspective in technology mainly comes from payments because I've been a very long-time believer that probably that's where our biggest risk is. If we lose our account relationship with our customer, we really have lost the foundation of our franchise.

So I really got interested in it, and we were very early in check imaging. We actually sent the first Check 21 Fed Forward file; it was an easy business case, and we don't have very many easy business cases. We see things that are obvious that we know we need to do, but when you put the numbers to it, at least in a short term, it's hard. So if we can make the numbers work, and it's obvious, and it pays for itself, we call that a good business case. If it's something obvious we know we need to do and we don't know how we're going to pay for it, we call that a strategic case, and we have more of those than we'd like.

We were very early in originating ACH because we believed electronic payments were where we needed to go, and when I say early, in the early '90s. And then I was on an ASHA course, so I got really focused on the same-day ACH. And I would challenge our industry that we sit here and we worry about the nonbanks taking over our business, and they are doing that in some respect on the payments, some respect on the lending. But in September, we're going to all have to be able to settle and receive a same-day ACH. It's just really disappointing to me that we call ourselves independent banks, we call ourselves community banks, and we're going to do that because it's mandated, and I think we can do better than that. We have to help ourselves a little, but the good news is in September I'm going to be able to originate a same-day ACH and whether you want to or not, you got to settle it. And I guess that's progress. So that's kind of our deal.

We're virtually 100 percent employee-owned. It's an ESOP [employee stock ownership plan], and that's something we worked on over the years, and we started out at a very low percentage and over time just accumulated ownership. So we're pretty proud of that. That's something I'd encourage folks to at least consider as you wring your hands on how you're going to raise capital because there's a lot of tools there that you can do with an ESOP. So I'll leave it to Mike.

MR. SEIFERT: Okay. Thank you very much. My name is Mike Seifert. I'm here from Fiserv, and I just sense a little bit of pent-up aggression or something. Let's get our shot to beat on the core

processor. So I guess I'm the lucky one who gets to be here for that, and Mark said he'd try to protect me as much as possible. As a result, I'm mostly concerned here about saying something that's going to get me in trouble when I get home considering the audience that we have here. I've been at Fiserv for seven years in a technology risk-management leadership role, and ten years of my career prior to that were all in technology, consulting, system implementations, and just a little bit of everything in technology.

My roles at Fiserv have been in the development of programs for managing risk, managing technology risk, implementing new programs, and also helping to push out risk management practices, information security practices in cyber security-education awareness training and other practices like that across our entire organization, across all of our businesses. So it's been a very interesting place to be and a very fun and rewarding place for me as well.

My current role right now, I'm serving as our chief risk officer for one of our divisions, and that is the division that focuses on our output products, the secure card production, any of our statement production things, and stuff like that. And this business is about half healthcare and about half financial services. So I live in a regulatory compliance and audit hell every day, and part of my expertise really is trying to streamline that, and do that a lot better through process and through people.

Usually when I go places I get to talk about cyber security things, and I mention Fiserv, and they think that we're a drug company. So I'm really kind of happy here that people know who we are. We service one out of three U.S. financial institutions as their core processor. We service about 135 million direct deposit accounts, and they're pretty large-scope across the industry. So it's an interesting place.

Thank you.

MR. MOYLAN: Well, let's go ahead and get started. The evolution of technology is certainly something we've talked about, and my personal evolution just with the FDIC started in 1980. Back then I was issued a manual typewriter and was still examining banks that had posting machines. So things have certainly changed.

But if you really think about it, the first smartphone was issued in 2007. Not that long ago. I'm going to ask my panel if we go back ten years in your career in banking and as a service provider, what technologies have you employed that have helped your business model, particularly in the acquisition and retention of customers or even operational efficiencies, and what have you learned through this process that's been very accelerated over the past ten years?

Shaza?

MS. ANDERSEN: Well, I would say that online banking technology, remote deposit, all of those services were not available to us many years ago, and if they were available, customers were very wary of them.

Now, fast forward 10, 15 years, we have all the millennials that can't stop using their smartphone. They're hooked to it, and technology has become very easy, and it's made it convenient for everybody to be able to do business and to do their banking. So I would say for us it's really helped us compete with the bigger banks because all of a sudden, the customer didn't have to drive to our locations to be able to do their banking. They're able to do it behind their desk.

So convenience, I think, I would say is a huge part. The other part is the access to information. Where before you needed to call people to get information, right now it's right there, all right in front of you, and you're able to get access to information a lot easier as far as I'm concerned.

MR. McCURRY: Yeah, I would agree with that. I think every bank in here, you might be different sizes, but almost all of us in our communities have one or two of the larger institutions that have more branches than us. And one of the challenges of community banks is how do you compete when they have to drive by two Bank of Americas and three Wells Fargos to get to you.

Years ago, we used to use a car courier service. We said, "Well, we're far away, but we will send a car to pick you up to get your deposits." So the remote deposit capture was just a phenomenal way to eliminate the need for the car delivery service. And I think it's also reduced the challenges of not having the branch network that other banks have. And, you know, we're not open on Saturdays. Some larger institutions are. But with the mobile devices, it mitigates a lot of the needs for doing it. So I think it's been a great neutralizer for the community banks and the big banks, and I think it will continue to help us compete in the future.

MR. STEEN: Well, once again, we saw the mobile banking and the remote deposit as a need, an obvious need. But we were struggling with the business case, and because we know what it costs us for a remote-deposited check by our core producer or core provider, but getting that cost passed down to our customer is a whole different matter. And so we're really struggling with the pricing process, because folks really do want it to be free. They expect it to be free, and they have very little tolerance if it isn't there when they want it and in the form they want it.

It's unavoidable. We need to stay ahead of it, but the expectation from the customer has gotten to be a real challenge for us. Patience level is very low, and they want it when they want it, and we need to be able to deliver it to them. So far I think we're doing a pretty good job of that, and at least as a community bank, we can at least look them in the eye when we need to and get them to where they need to be. I think we all have that same kind of challenge.

MR. SEIFERT: As Bob said, the continued evolution and adoption of bigger, better, cooler technology is inevitable, and there are three factors that I keep hearing over and over. There's one of keeping up with expectations. You want to have the coolest things, right?

We have this millennial factor, and millennials being the largest generation in the U.S. right now, and it's the first generation that's been larger than baby boomers and one that's poised to inherit a ton of money, and there are all kinds of other factors there. So everybody wants to attract this kind of group, and this is very interesting because they think so differently. I'm slightly outside of that generation. I don't get it. There's a lot of things I don't get, but I know that the influences, the way they think is very real, and it's very real in our business, and if anybody's going to our client conference in a couple of weeks, you're going to hear about that a lot. All of them I've been to for the last couple of years, they talk about that. You know, things like I have people on my team that are considered young associates, and when I'm reviewing their expense reports and looking at it, I'm always like, "Why don't you rent a car? You've got to drive so far when you go to this location, why won't you rent a car?" They won't do it, but they'll do Uber. I just don't get it. It's things like that. But it's very much different. So when you have a cool technology thing, it's so important, and they're influential as well. They're influential to their parents, to their grandparents. They set a cool factor that other people need to copy. So staying on the cutting edge of that technology is very important there.

Also there's the factor that Mark brought up of operational efficiencies, and the numbers that we see and the ones that we talk about are doing the transaction in a branch costs roughly $4.25 versus doing a mobile transaction costs about 10 cents. Lots of opportunities for efficiencies, and also what we're seeing then is branch banking transactions are continuing to go down while online transactions are continuing to go up. So there's a lot of interesting factors going on there.

MR. MOYLAN: I'm going to add a little quick follow-up question to this. You know, particularly in certain parts of the country, with rural depopulation and kind of the mobility of the population, are you seeing any changes because of the technology on your retention of customers once they've started that relationship with you? And I'll just open it up to the panel.

MS. ANDERSEN: Well, I would say that definitely. I think that the more we make it convenient for our customers, the happier they are and they're not going to want to leave you. I think the one thing I wanted to add to what Mike was saying about the operational efficiency, I mentioned earlier that, you still need the branches. You still need that brand. You still need them for deposit gathering. But from an operational efficiency, it used to be where, I used to have branches that were 5,000 square feet with 10, 12 employees in them. Now I have branches with 800 to 1,000 square feet with three people in there. So I think it really has helped also from an efficiency standpoint to be able to have the visibility, to have the brand but not employ as many people as you needed to employ, because customers are doing everything on their own.

So, I'm answering your question sort of in a roundabout way. I would say the more convenient it is to the customer, hopefully the more retention, but you're talking to community banks, and I really hope that our customers are with us because we're able to provide them the service we're able to provide them, and technology can't provide that. It's the people.

MR. McCURRY: I've got an interesting take on it. Again, I think we're a people business, and at the end of it, that's got to be what we drive with, but technology so much complements it. A couple of examples. My father called me recently, and he says, "Hey, your bank's got mobile banking, doesn't it?" I go, "Well, yes, we do now." Now, my father still has a flip phone in his car that he keeps in his glove box, and he only turns it on when he needs to make a phone call, and he turns it back off. But it was important to him that we had mobile banking. So, I was like, "Well, why do you care?" He goes, "Well, just I like to know that my bank has these things." I think, though we're in a contracting business, contracting industry, I think the success we've had is letting people know that we're committed to the future. We're excited about the future.

When we took over the bank three years ago, we raised our capital, almost doubled it, and did it with local shareholders in Florida, which was unheard of in late 2012, 2013. And what we had to articulate to them was that community banking was still a good model, was still going to be there in the future, and we were going to be as well, and a lot of the discussions were about what kind of technology are you going to embrace.

We just had our second capital raise. We completed it last month, and part of the presentations to the shareholders was about technology, and that was the presentation and the follow-up questions are: "What are you going to do? What are you going to be able to offer in the future? How are you going to be as advanced to bank with as some of the larger institutions?" And I think some of these people won't actually use the services, but they like to know that you're committed to the future. And so I think it sends a signal to not only just your customers but, again, in our case, certain shareholders. They wanted to know that we were going to continue to embrace technology in the future.

MR. STEEN: We do have a segment of customers that have moved away. We are in a rural area in Iowa. We do have a stoplight in our county. It allows them to bank with us, and they want to bank with us. They make a point of trying to bank with us. And without these mobile remote deposits, without the mobile banking, without the infamous debit card we all have, technology gives us a chance to keep those vehicles, and it's pretty rewarding. We do have a segment of professionals, young people that have moved away and remind us that they still bank with us and that they have other banking relationships and our products and services are at least as good and many times better, and that's all because of our adoption of technology.

MR. SEIFERT: So, a quick follow-on question to that point, and another factor I didn't point out was the convenience factor. We have evolved to a culture where we want everything now. Anybody use Amazon Prime? I was a late adopter there. I just signed up for it not too long ago. I buy so much stuff on Amazon Prime it's just ridiculous right now, because I get it right away. It's kind of cool. My wife was getting really annoyed. I'll probably have five more packages sitting on the steps when I get back there tomorrow. That's how we are. We want to get this stuff right away. Raise your hand if you offer instant issue of your debit cards in the branch, you know, another interesting technology enabler. Why go and send your orders off to have cards manufactured and then mailed to your customers when they can open an account and you can give it to them immediately?

Those are expectations now, the expectations of remote deposit capture and also capabilities for doing things like instant payments. I mean, I know we're doing instant real time person-to-person payments now. That's just the direction everything is going. Instant gratification is key in almost every one of our industries right now.

MR. MOYLAN: I think the next phase really we should talk about is how new technology factors into your strategic planning, particularly at the board level. I'm the regulator here, and you folks are the bank. You have a lot of people coming to you with new products saying, "We've got the latest bell and whistle. This is going to satisfy this need in your customer base." Really, from a board perspective, how much is available technology or your current technology considered in your strategic planning, particularly, as we mentioned this morning a lot, having to do with your new customer base, the agility of the community bank? How is that factored into your board discussions or strategic planning, if it is?

Shaza, would you like to start?

MS. ANDERSEN: Sure. Well, again, whenever you're thinking about your strategic plan and you're thinking three years ahead and you update it every year, IT has become a major part, just like deciding that you want to grow or deciding that you want to open branches or deciding that you want to add certain products. IT is an area that you can't live without. I know that if you tell me three, four years ago we had one IT person that was serving our bank, right now in my head of information securities here, George, we have what, seven or eight people in the IT department now? Nine people in the IT department, and we're a small bank still. So we have built a lot of infrastructure to be able to meet the ever-changing and ever-demanding technology that we're being faced with.

From a board level, I think the board is sort of similar to Neil's dad. They want to know that we offer it all. They want to know that we're taking care of our customers. But, more importantly, I think the biggest thing that's been happening in my board room is it's all about security of our system. It's all about the cyber attacks that we've been experiencing. Our area right here, MedStar, a hospital right here in Georgetown, got ransom attacked. So this is starting to happen, and it almost happened to our bank. For ten minutes, I think somebody attacked our system, and our IT people were able to get in right away and stop it, and when we got the call, I think, you know, George told them forget it. But it's happening, and it's happening to a lot of people, and it's in our back yard. So that's the main area that I think has been troubling to me and to my board I would say in the last few years.

MR. McCURRY: Yeah, I think we've done a tremendous amount in the last 36 months. After we raised our new capital and really re-kick-started the bank, in the first 12 months we got rid of all of our old servers and went to virtual servers. Twelve months after that, we made the decision to completely convert our core data processing and item processing system to another system and also start offering different ancillary services.

So we've done a tremendous amount in the IT area, technology area in the last three years, and our board has been very involved, and part of the original plan was that we were going to embrace this and that we were going to do these things. We were committed to our future, and this was a part of what the future was.

That being said, we had to be very concerned about the security part of it as well, and we've been very focused on cyber security and technology. And, in particular, I was on a conference call with Doreen Eberley. I think a couple of years ago Doreen put on a conference for all the CEOs, and her parting message was, "Listen, everybody, this belongs on your desk, not your back IT room's desk." And I listened to her words and actually reached out to her and sent her a message and told her that I enjoyed it and we'd like to play a part in helping out with the FDIC, and I've gotten very involved with the FDIC, the OFR [Department of the Treasury's Office of Financial Research], and the state of Florida with cyber security issues and getting involved with it all.

And, in fact, last night I was at a reception, and I was talking to Don Satzinger. He's one of the head IT examiners. And I was telling him, I said, you know, "We talk to all the examiners all the time. I'm really committed," and he thinks I'm just kissing up to him because I was just, you know, trying to get up with our examiner. I was telling him, for example, I said, Mike Dean, he's the regional director for the southeast United States, and every time I see him, I go, "Hey, Mike," and I go, "Neil McCurry." And he goes, "Yeah, you're the guy who loves IT," and he's looking at me like I'm just, you know, kidding him. And, just coincidentally, Mike Dean came walking in the room, and he was like, "Well, hey, there's Mike Dean." I go, "Hey, Mike, Neil McCurry." He goes, "The IT guy, right?" And so I go, "Yeah."

I mean, the point is that we have tried to make sure to stay abreast of all the emerging risks. We work very closely with the regulators, talk about what we're doing, ask for advice as well, and believe there's a great opportunity; but with that opportunity comes a great responsibility, and our management and board are very committed to stay in tune with that.

MR. STEEN: We rolled our proof machine out of the building in 2001. So my board asked, "Okay. What are you doing now?" We live and breathe the security. We think about it all the time. We worry about it all the time. We try not to overreact to it, but, you know, we promised Mark that we wouldn't get into configuration, and that works good for me because I don't do that.

But our board does understand that we have to stay current, and they're used to it from our small bank perspective. So there's a certain element of trust that when we take something to them, we give them our best shot at why this matters and what this is going to cost and what our best hope for our business case is. We usually get an endorsement.

MR. SEIFERT: Given the number of financial institutions that we support and the number of you that we support, security and technologies, basically we are a technology company, but it's obviously a top board priority.

Our enterprise risk function is an oversight function that's responsible for anything related to security, incident response, availability, resilience, any of these things that actually fall into this technology area. Our function reports directly to the Fiserv CEO. It's that important, operates as an independent function similar to a corporate audit function would in a large corporation, and it's also a very powerful function. It's a very powerful function to make things happen, make sure we're doing security right, make sure we're staying on top of things, not cutting corners, because what happens is you guys were getting pushed as soon as we do that, if we were to cut corners on any of those things, not keep our systems up-to-date, not have solid practices, we would be putting account holders, all your consumers, all of you as clients at risk. We think about that every day. When we talk internally, we talk about how many millions and millions of account holders we support. When I talk with my teams, I tell them that anything that we're doing, we're doing for our own benefit as well, because lots of our financial services and lots of the things that I do personally, they're somewhere in Fiserv's systems. So I'm doing that for the sake of myself as well. This is definitely a very top priority for us.

MR. McCURRY: I think also what's helpful is that everybody out there has read and seen the press about Target, all the different types of IT breaches out there. This isn't news to anybody. All of our boards are aware of this risk, the world we live in.

What we really have to do is decide how much it is going to cost us, how are we going to incorporate these costs into our operating structure and still maintain our profitability. I don't think from the board standpoint, I don't think anybody has a challenge articulating to them that there is a real cost and real risk to cyber security. It's just how are you going to appropriately address that security.

MR. MOYLAN: Well, I think that's a great point to follow up. Bob, you had mentioned too as far as a business case, you know, is it really necessary for our institution. I'm kind of going to leverage off that. Really, as far as the decision process that your institutions talk about, sometimes you can put a number to it, sometimes you can't. I'll ask you to start, Bob. How do you go through that decision process of whether to acquire a new technology and to deploy it? And maybe talk a little bit more of your example of obviously your business case analysis.

MR. STEEN: Well, we've been a beta bank for multiple projects, and so some of my peers would warn me about being on the bleeding edge, but I would argue that we've been pretty lucky, I suppose. So, as a beta bank, we got in the game pretty inexpensively. Some of those business cases were pretty obvious. Check imaging was one. I remember giving this guy a check for my first check imaging product, and he walked out the door, and my operations officer said, "Are you nuts? He doesn't even have a license plate on that car." We've taken some chances. It was a rental car. It was okay. It was okay.

We do have providers coming to us with ideas, but I'm focused on payments. So, I've been involved in the payments world, and I've seen some of these things coming well before some of our vendors have offered them up. We kind of knew where we needed to go. It is hard to take

that contract and look at that number, look at the annual maintenance, and pencil out a business case because, again, our customers, you know, when they download an app on their smartphone, they're getting it free, and that's kind of what they expect from us, and it's getting very difficult to make everything that way.

It's a constant struggle, you know, particularly when you have the security levels on it that we know we need. We just work through it, and for the most part we've been lucky. Most of the projects we've done have worked. All of the beta pilot projects have worked. Not all of them have been adopted, but just because of a scalability issue. But we keep trying.

MR. MOYLAN: Anybody else want to comment on the business case analysis?

MS. ANDERSEN: I would say that our latest IT product, if you call it, was taking the deposit via your phone, taking the picture. We were one of the first people that signed up with Fiserv. Fiserv is our core processor.

The process that we go through in order for us to employ technology is very extensive. We have an IT committee, we basically vet all the pluses and minuses and then take the cost into consideration and if half of our customers are going to use it, it's worth it. If you're going to have one or two people that are going to use it, it may not be worth it.

We really do study it. We study the vendor. We're limited a little bit because, again, we don't process everything at our bank. We do use a core processor, but they've been using up-to-date technology and bringing it to all of their institutions. So I would say we've been very pleased with the technology that we've been able to adopt because, again, it has made it more convenient and nicer for the customers. Right, George?

MR. McCURRY: You know it's interesting you say that because you mentioned that using the flash capture that you were one of the first ones to use it, and I think that that's a great technology, but it's come to the point where almost all of us have it. It's like the ATM. You don't differentiate yourself with it anymore. So we also try to look at what's coming that not everyone's using so we can differentiate ourselves. I personally like the P2P [person-to-person] payments, and it hasn't been very well adopted, but I think if you can get out there and have it and articulate to someone about why they'd like it and get them using it, it's a way of building some brand loyalty with your customers, as opposed to waiting until everybody else does it and only do it because you have to because everyone else does.

So you have to pick wisely on that and certainly choose your vendors correctly, but I think that is part of the challenge. And the excitement is really trying to understand what the next trend in the banking industry is and trying to stay a part of that.

MR. MOYLAN: Mike, can you talk maybe from a service provider on what you do looking down the road? I mean, obviously you listen to your client base. You try to stay in tune. Strategically, from your service, how you try to figure out what your clients are wanting and what may be next.

Obviously, as Shaza said, with being able to take a picture of your check, that was something that you folks provided. How do you look down the road?

MR. SEIFERT: There's a number of different ways of doing that. I mean, one is just constantly monitoring the market. There are so many other companies out there that are outside of the banking world right now that we're kind of looking at disrupters to our world and all the different companies entering payments. What's interesting about all these companies, too, is the amount of brand loyalty they have and the amount of brand trust, and the studies that I've seen and the studies that we frequently talk about as to when you look at a lot of these like Amazon or even Costco, you know, names like this and Apple, the trust and the value in that brand is a lot higher than a lot of major banks.

So, what happens when they start offering those kinds of services? We need to constantly be thinking about that and looking at the stuff that's coming down the road. But we also have a lot of experience in that since we have about 700 different products and services that we offer in this area, there's a lot of opportunity just in terms of integration for improvement and for innovation. We integrate this with this, and you do it a lot easier; or integrate this to this and this and then be able to put analytics on top of it; or better customer relationship management; or all these things—do this integration better across all these products. That's another kind of innovation that is a big improvement, that's really very difficult to do, and very IT resource-intensive if you're going to do it on your own. So that's another area of innovation that we're constantly looking at.

We frequently met with different working groups like our signature users group or one of our premier user groups and things like that where we actually get together with bank leaders to hear what they're asking for and talk to them about that. There's a lot of very interesting products out there.

MR. MOYLAN: I guess it's probably time to talk about risk management and managing this IT risk. Neil, you talked about the cost. Shaza, you said you had one employee. Now you have nine. I guess from the technology you currently deploy, what keeps you up at night? What's probably your biggest area of frustration as far as managing this? What are you most asked about by your board of directors?

And I'll start with you, Shaza.

MS. ANDERSEN: Well, this is an area that's really near and dear to my heart. I think cyber security, the more that we try and protect our systems, there are more people that are trying to hack into our system. We get regular reports at our bank on how many attempts are going against our bank system. We have 800,000 attempts a month at our bank of hackers that are trying to get into our system. That's huge for a small bank. We're not Bank of America. Eight hundred thousand attempts per month on average at our bank of people trying to get into our system, and I think we try and mitigate it as an organization. You have your insurance that could help you if you have an incident. You educate your employees. You try and educate your

customers. There's always something new that's happening, whether it's wire fraud where somebody e-mails you and asks them to send them your account information and the customer doesn't pay attention that while it says it's coming from Shaza Andersen at WashingtonFirst Bank, it's really coming from somebody else.

There's just so much that's happening in our market of cyber fraud that really concerns me. And my plea to my regulators and the government is to really educate the consumer specifically.

I'm going to share a story with you.

I was at a friend's home where she didn't have any security to her computer. Well, if you don't have security to your computer, my 15-year-old could go in and find out all your passwords. Well, you have to protect your computer. I mentioned to Mark over the phone, "If I'm a thief and there's a home that the door's open and nobody's guarding it and there's a home that is locked and there's an ADT sign on it, which home am I going to go to first?" So, with that, I said, "Well, you have to protect your computer." She said, "Oh, don't worry about it, if somebody gets into my account, the bank will cover me." I said, "The bank is me! It's my clients. It's my customers. It's my shareholders that are paying for that." I really think we need to have an education to all our customers to be able to say if you want to do online banking, if you want to be able to use your computer to access your money, you have to secure it, just like you secure your checkbook.

And so that's an area that I think is evolving, and I really hope that we'll continue to see more consumer education. The business customers, they understand it a little bit better, but the consumers that are there that really have no business of logging into an account, they're leaving all their information free out there for anybody to get into their system. So, that's an area of concern.

MR. McCURRY: I remember 16 years ago at my previous institution, I stood at our shareholder meeting and we were just rolling out Internet banking, and I was telling everybody, "It's great, but you've got to be careful with Internet banking because right now there is a 14-year-old kid sitting in some house in Eastern Europe, and he's trying to hack into us and hack into your systems."

A couple of months ago we had a shareholder meeting where I talked about mobile banking. I said the difference with technologies is that it used to be the concern was a 14-year-old in Eastern Europe hacking into your system, and now the concern is the whole Chinese government is trying to hack into you.

The bar is raised quite a bit, and we have to adapt to it as well. We're very focused on making sure we understand the risk. There are a few schools of thought. One is that the public is so desensitized to breaches that it's not an issue, and, maybe that's true. I probably have the opposite view. Banks, specifically, community banks are held to a higher standard than say Target or someone else. My concern is what happens to your reputational risk and that there's a

slow deep bleed, there's a loss of confidence if you have a breach, and you'll never know about the customers that you don't have that you would have had if it hadn't happened, and literally, the vitality of your organization can be greatly diminished or you could stop to exist over time if you have a breach.

So, I'm very involved with it all for those reasons. I tell our staff, when we train, that somebody could come in and steal all the money out of the vault, all of it, we don't want anyone to be hurt, but at the end of it all, it will be a bad month for us. That's about it. A cyber event could really be a knockout punch to the whole organization. I hope that's not the case, and I hope that maybe if anything happened, that its people are desensitized to it, but I think we all have to be very careful. Not only do I need to be careful, my shareholders from our bank, we need to make sure that we don't have a breach so your customers don't lose confidence in the community bank model as a whole. I think we all have that responsibility to each other.

MR. STEEN: The information we see more these days is that most of the risk is coming from just human mistakes, things that we do that we should know better than to do. Most of the bad viruses are coming in through e-mail, people clicking on something that they weren't thinking, and all the sudden you've got a big problem.

So we work really hard to educate our staff to think about what it is we are doing. Even if it looks like it's for me, it may not be. Just be very careful, and if you have a question, there's a way to scan that for a virus. Take a minute, do it. You know, our biggest risk, I think, is losing trust with our customers, and trust is critical to everything we do. So we're very conscious of that.

One of our worst nightmares would be if our customers opened a website that looked exactly like ours but it wasn't and they had a problem, no matter what you tell them, they saw us on that website, and so we did adopt a .bank domain. The ICBA [Independent Community Bankers of America] and the ABA [American Bankers Association] have been working really hard on that, which it has a very strong security nature, and I'd encourage you to look at it. It gets pretty deep into your system, but I think it's worth it. As an industry, we need to do that.

So we just constantly work at it. But we try really hard to get into our schools for some sort of education. For young people, it's very difficult. They have the curriculum. They don't want their day messed up. You know, it's inconvenient. So it's really hard to reach out to these folks and talk to them about the basics of not only security but just handling your finances, and I know you all experienced that.

So we keep trying, but security is everything, and we don't get a pass from our customers if their information is breached.

And one thing we're fighting is, without mentioning any names, Visa and MasterCard have trained my customers that they have no liability. I mean, that's a big deal, and it continues to get worse. Visa just passed another rule that a merchant cannot ask virtually under any

circumstance for an ID of a cardholder. So our customers know that they're not going to have a big liability. So, their caution antenna is not as high as it should be.

MR. MOYLAN: Mike, before you go, I'm going to kind of change the direction. After I ask Mike this one question, I think we'll get set up to take a few questions from the audience.

Number one, I wanted to mention first that Shaza brought this idea to me regarding consumer awareness, unsolicited. However, in your packet I believe there are brochures that the FDIC, in fact, I believe last month, we published our consumer news, and the entire consumer news was related to customer awareness in relation to cyber hygiene and what they can do to protect their information, and I believe in your packet you will see one brochure for your business customers and a brochure for your consumer customers.

Shaza's absolutely right. There are two legs to these transactions, and particularly as far as IT security, and certainly that one leg is your customers, and that is something that we certainly strive and recognize through that.

Really from your perspective, Mike, you know, my role is twofold. I have supervisory responsibilities over the TSPs and also the banks here in the audience here today. What is your company's role in providing assistance to the clients there and their IT risk management obligations? And I know we've talked about it, audit and various other concepts, what are your frustrations, and what efforts are you trying to do to satisfy some of these customer needs as they try to manage this risk?

MR. SEIFERT: As we're talking about cyber security, there's just so many points here, I'm going to probably jumble those up quite a bit because we talk about this quite a bit. When you talk about cyber security, there are just so many moving parts. It's very difficult for any organization. It's difficult for even an organization as big as us to maintain security and be on top of it at all times. It takes lots of talent. It takes lots of resources, lots of time, and it takes a lot of doing projects, the kind of projects people don't want to do, the things like not inventing sexy cool new things but, rather, going back and updating, fixing, patching old stuff that's in place so that you can actually move on. So this is very resource-intensive, and one of the benefits of outsourcing is that you kind of do outsource a lot of that, and at the levels of IT staff that a lot of you maintain, it would be very difficult to have the right kind of information security and technology talent to be able to stay on top of this stuff and doing application development, doing the right kind of coding, staying on top of all the different security frameworks and compliance requirements and things like that.

That's something that is definitely outsourced to us in many circumstances. Also things like PCI [Payment Card Industry] compliance. We spend millions and millions and millions of dollars on PCI compliance, and it's a big thing if you're a customer of ours, lots of times you don't have to worry about those things as well. So I think that's another piece that could be outsourced there.

Also in terms of doing some of the things from a regulatory standpoint, the reports that we create, the assurance things that we do, the SOC [Service Organization Control] reports that we create, and the attestations of controls that we give to you to share with your auditors and to share with your assessors, I think those are other things that we're kind of doing for you as well. A problem that I'm finding is that the burden of compliance is becoming very large, and I have a large team right now just in one division, just trying to keep up with compliance requests and audit requests from the third parties that are auditing us, including clients.
I think we service about 4,000 clients in our division, and every one of them comes to us with a new, better way to do vendor management and a new, better questionnaire. All of them are the same questionnaires asked over and over again. There's like the same 100 or 200 of them, but you've got to do everything more on a one-off. It's very difficult. We're really working to try to develop much better materials so that we can be much more streamlined in helping you to meet your requirements for effective vendor management. We're doing that by trying to do better third-party assessments, more robust third-party assessments, putting those in a way that you can better understand them and leverage them. So I think that that's something else that we're trying to do in order to really help out in that area.

I'm not sure if that was really answering.

MR. MOYLAN: No, no. I think that's great. Go ahead.

MR. SEIFERT: One other point that I think is important, especially at this level: there's a lot of talk about cyber risk. I like to look at this in four different areas if you break down cyber risk, and when I talk about these, inherent in each of these should be rather obvious, but we tend to look at these in terms of risk of availability. Is the system available or not, are your systems resilient, can you recover?

Also, the second one is accurate money movement, obviously a very big concern. It's a huge concern for us. We move a trillion and a half dollars a year through our systems, but that goes to the integrity component of this. Then also we have the one that everybody talks about, which is our information-exposure risk. We hear about the Targets, all the other examples, what happens when you lose that risk.

The fourth one now is kind of more emerging. We are starting to talk about it a little more, and that's the data destruction risk. By data destruction, these are the things we're seeing related to ransomware. This is getting very prolific. This ransomware problem, it is very scary, although as we were talking about last night, when you have a ransomware problem, I think lots of places don't generally have it twice because it is so painful. I mean, somebody opens something they shouldn't open up, it encrypts your data and you can't get it back unless you pay for it, unless you have good backups. It's often a very good lesson to people who aren't backing things up very well.

So, if you kind of look in those four different dimensions, you can assess your organization and say, "Here's where we need to do things better. Here's where we need to improve. Here's

where we need to see what our service provider is doing." And I think that's a good way to look at cyber risk.

MR. MOYLAN: You know, first of all, I would appreciate a round of applause for the panel. This is a very tough subject, and I greatly appreciate your time. Thank you.

I have a unique perspective in the fact that I spent the majority of my career as an examiner in the Midwest, and so I've been in a lot of the small community banks. I understand community banking, and I've been in larger institutions. My goal of the panel is not just to focus on the risk but the opportunities of technology, and that's why I appreciate Bob's comment, particularly in those smaller communities that are able to retain customers in those areas.

It's really a double-edge sword. They're great opportunities. Me, as a bank customer, what I can do now in managing my finances, making sure my college kid isn't spending $35 for a cup of Starbucks, and moving money around very quickly on a phone call, I greatly appreciate that. Of course, when I put on my hat and I come to work, I have the other side, which is worrying about risk.

So I think, really, the context, as you can see, as we've talked about today, the evolution of technology and really where we've come and what those opportunities bring to you in the room and balancing that risk, understanding that risk, managing that risk, when visiting with my panelists, what I'm probably most excited about is how fluent they are in cybersecurity now, and that's certainly been a goal of us all is to recognize that risk. But the innovation and the possibilities, again, what the next ten years are going to look like and the opportunities for this group certainly excite me.

And, with that, I would be happy for the panel to take any questions.

MR. ACKMANN: I'm Steve Ackmann from Highlands State Bank in Vernon, New Jersey. We're about ten years old. When we built that bank, we got servers everywhere, in the basements, and new branches, and a lot of those servers are starting to die now, and we keep talking about moving things to the cloud, and I'm kind of wondering from a regulatory standpoint or maybe some of the other panelists, where your thought process is on this stuff right now. It seems like there's a great business case there. It seems like a great business case here, but where is my data? I don't really know.

MR. STEEN: Yeah. I'll start with that one. There is no "cloud." It's a data center somewhere else. And so I have people come in, and they try to sell me services, and there's probably a really good business case for it, but I tell them, "If you say cloud one more time, you have to leave," because there is no cloud. It is a data center, and in our small world, we went to virtual servers, and we got fiber optics between locations so we can now do replication every three and a half minutes. So there are alternatives, but you are handing your data off to somebody else.

MR. SEIFERT: We are very conservative when it comes to any of that. We've been very resistant to utilize any computing infrastructure that's outside of our control, for obvious reasons. Where is your data? What do those companies allow you to do with it? What kind of protections do they allow you to put in place? If you're going to a regular cloud service provider, they want you to put data loss prevention monitoring agents on all your end points and your servers or put in certain types of other monitoring technologies on their networks. What kind of audit rights are they going to give you? There are so many questions to be asked there, and lots of the problems and a lot of the questions come down to this: What are you really held accountable to do to ensure you have the right kinds of security controls in place? You have all the controls within the FFIEC [Federal Financial Institutions Examination Council] Handbook. You have PCI data security standards and many other standards. How can you ensure a lot of those are happening when it's actually at a third party? How do you know that they're in the right places and you actually have effective coverage and effective controls in place? That's where it really kind of starts to break down. That's why we've been very conservative on what we do there. Where we've utilized any third parties for any types of data storage or any types of off premises things, we're very diligent. I think the legal process and the contracting process is probably the most painful piece of all that, but we're very diligent on what we have to do there, have to have the capabilities for the right types of controls in place. So it's kind of a scary thing. If I think of all the institutions that I work with or all the institutions and healthcare organizations, whoever else that has my personal data, and they're just, you know, "Cloud's good. It's nice and cheap. Let's do it." Where are they putting all that stuff? It kind of bothers me.

MR. MOYLAN: I think from a regulatory standpoint, it's an emerging issue, and the cloud is as fluffy as the term "the cloud" is because there's a lot of different nuances to what is in the cloud or what a cloud is. We have shared application types. If you take a look at TurboTax, I can download it. I can store my data there, or I can just log in and use the software. That's a version of three different services under the cloud. Certainly part of the business cases Bob talked about is a key component, understanding what you're getting, your rights, the contractual nature to really build a business case, the cost benefit to those type of things.

Next question, please.

PARTICIPANT: Michael, you said some interesting things, and I don't know if everybody caught those, but that the millennials are now the largest living generation in this country, and the other thing he said is they're waiting to inherit the baby boomers' money.

MR. SEIFERT: That's a lot of money.

PARTICIPANT: There's a lot of us in here that fit that profile. And the problem we have is, you know, the next thing he said was bank branding versus tech branding, Amazon, Apple, Google. How many people know what a Google Wallet is? How many have a Google Wallet? Do you know Google Wallet is now FDIC-insured? Anybody know that? I got it right here. Google on your phone. "Google Wallet, now FDIC-insured." And it's a pass-through. I'm assuming nobody in this room has the Google Wallet account. But if our kids think that they can get their accounts

and they get it for free from Google, when we die, we better call our attorneys and get our wills changed because we're going to have to wire our money to Google Wallet. So they're ahead of us. We're playing catchup baseball, and we better pay attention because our competition is way ahead of us in trying to get the money out of the banking system. And we need technology to make sure that doesn't happen, and we have to embrace it, not fight it. So it's not a question. That's just a statement, but I thought you all needed to know that.

MR. MOYLAN: All right. Thank you.

MR. CALABIA: My name is Chris Calabia, and I'm a supervisor from the Federal Reserve Bank of New York, and this panel, like the prior panels, has been terrific. So thanks to our bankers for being so candid and our service provider as well, and thanks to our colleagues with the FDIC for organizing such wonderful panels.

I wanted to bring up a question that Michael raised, and that is that you mentioned as part of vendor management, you got all these questionnaires from bankers. The first question I want to ask Michael is: Is there a question that you think bankers should be asking you that they are not, and then maybe for the bankers, what question do you find your IT service providers get stumped on?

MR. SEIFERT: Well, I can't imagine there's a question that hasn't been asked. You know, I've been reviewing the last couple of days an updated version to our division SIG document. Anybody familiar with what that is? It is the Standard Information Gathering questionnaire. There are 1,800 questions related to your information security and controls posture. Within 1,800 questions, most things are generally covered, and the purpose of that is to actually say, when somebody asks those questions: "Here's our SIG. Take a look at it. Whatever question you want answered, we've got an answer in here." Oftentimes what we see, and I think one of the problems is, the vendor management activity itself is the check-the-box activity. So a policy is developed and an approach to vendor management is developed. You have somebody with a vendor management role, and they say "I need to do this," and then they check the box. "I need to do this, and then I need to do this."

So when you come and you get stuff, we have to have SOC reports to give you. We have to have SOC reports. We've got our SIG document, and we have all kinds of other client-assurance documentation. Lots of times I don't think it's ever even looked at, because I think what's defaulted to too often is that there's a checklist of things we need to do in order to do vendor management; "This is what our policy is." And if it's not in this format or this thing, then it's something I'm not going to accept.

What that does actually, is that decreases the kind of information that you're getting. You're getting a lower quality of information. You're getting information that hasn't been vetted as much by third parties because you're trying to do a one-off assessment.

So what I would challenge this group to do is to think about that. Think about what you're asking. Think about what you're getting in return and how you can utilize that. My strategy, the one I'm trying to do, is to develop the best materials we can that are validated by third parties, be able to give that, along with our story: Here is how we do this, this is why this is done the right way, and this is why we feel that you should trust us, and here's how to utilize it.

I think that's a much more effective way to do this rather than grabbing a document, checking the box, and moving on. So that's kind of my advice there.

MR. McCURRY: And let me pass on some experience about vendor management of core systems, because we just did a core conversion in the last 12 months, and there were some comments earlier in the day that people had frustrations that their core providers were just being difficult to work with, and we did a conversion, went to another system, and what we were trying to do at first was just to hopefully get a better product and maybe save a little bit of money. And what I realized through that process is that I think these core providers are all worried because our industry is shrinking. So their customer base is declining as well, and it was a frenzy to get our business, and at the time we were a 100ish-million-dollar bank, and there wasn't a question that we asked for which the answer was "no," and certainly when we got the contract, it was 150 pages and you have to read through it all, but they won't change anything on the contract because they want to be able to tell the next person they've never changed a contract. They'll do an addendum to it all saying, you know, what's on page seven, that doesn't count. So but that's how they get around that.

We found them very receptive to all of our concerns, whether they were contractual, risk-based ones, or pricings. And it almost became like a game at the end. We were getting ready to sign, and I said I'm just going to see what else I can get them to get, and they catered my shareholder meeting at the end of the year. I signed the paper, and I said, "No, no. I want you to pay for all my food and drink in my shareholder meeting," and they go "Okay." It was six months of that as well, and, you know, I have the series of proposals as it went, and the things they swore they would never do up front they were happily doing at the end.

So, I would just suggest that if any of you have contracts coming up, even if you're going to stay with your provider, don't let them know that, and I think you have a lot more bargaining power than you think you might because of what's happened in our industry.

MS. BRADY: I'm Gwen Brady, and I'm the Director of Banking and Insurance for the Virgin Islands, and my question is really on the issue of the unbanked community. There are still many unbanked individuals, particularly in minority communities across America. Can you, particularly Ms. Andersen, can you discuss for us how technological innovations can help community banks reach the underserved communities?

MS. ANDERSEN: Well, being a community bank, we are very involved in our community. We have a lot of education. We get involved with groups that educate the people around us on how to bank.

Our first branch was in D.C., and D.C. has a lot of people that don't use banks. They use check-cashing places, and we worked with the D.C. Commissioner at the time, and we tried very hard to educate people on how to become bankable. I think a lot of it is hard for banks because there's the part where you want to bank everyone, but then there's the BSA [Bank Secrecy Act] that tells you that you have to identify them. And so if they don't have IDs they can't prove to you that they're who they say they are; then you can't open an account for them.

So we had some struggles because a lot of people, they don't drive. They don't have DMV [Department of Motor Vehicles] IDs. They don't have passports. So how are you able to open an account and not violate your BSA regulations? So I think that at the end of the day, we just really encourage people to learn how to go to the DMV and get an ID and learn how to open an account and learn how to balance their accounts. It's a lot of education I think in the underserved communities more than anything else, but we're a little bit handcuffed. We can't have anybody walk in and open an account without having the proper "know your customer" to go with it, or our regulators are going to come in, and they're going to say, "Well, you're not supposed to do that. You're supposed to know who they are. You're supposed to identify them."

So it's a challenge, and I think in D.C. specifically, they were thinking about issuing debit cards instead of checks to those types of customers that aren't able to open a regular account. How that panned out I can't tell you because they were working on it at one point. I thought that was a good idea to teach them that instead of taking that check and trying to go to cash it at a check-cashing place, to have a debit card that they're able to utilize at different places. But, again, I think they were having struggles with people accepting those debit cards. They didn't want them. They really wanted cash. So it's a challenge. But the education is all I could say or offer from a community bank to be able to help people.

MR. MOYLAN: I'm keeping it very, very simple, and it's not my area of expertise, but I remember being in a meeting where we talked about this from a purely technology standpoint, I think there was some analysis done by the FDIC about the number of folks who are unbanked who have phones, and with a phone, as we've demonstrated with the technology here today, you have an opportunity, and certainly the organizations and you folks have broadened that technology that there is an access point from a purely technology standpoint to banking.

We've run out of time. Again, thank you all very much. This is not the easiest subject. I promised you we didn't talk about firewalls.

Thank you all.