Transcript

Better conversations. Better outcomes.

Episode 43 – Protecting your practice: A cybersecurity roundtable

Paul Ewing - The part that advisors tend to overlook is with cyber security there's a technical component to that and there's an assumption that, well if I hire the right IT provider, I'm now protected. They should not have that, it's a false sense of security. And so what the advisor should be thinking about is having their own way of assessing risks and conducting a formal risk assessment as it relates to the cyber security risks for their firm.

Ben Jones - Welcome to *Better conversations. Better outcomes*. presented by BMO Global Asset Management. I'm Ben Jones.

Emily Larsen - And I'm Emily Larsen. In each episode, we'll explore topics relevant to today's trusted financial advisors, interviewing experts and investigating the world of wealth advising from every angle. We'll also provide you with actionable ideas designed to improve outcomes for advisors and their clients.

Ben Jones - To access the resources we discuss in today's show, or just to learn more about our guests, visit bmogam.com/betterconversations. Again, that's bmogam.com/betterconversations. Thanks for joining us.

Emily Larsen - Before we get started, one quick request. If you have enjoyed the show and found them of value, please take a moment to leave us a rating or a review on iTunes. It would really mean a lot to us.

Disclosure - The views expressed here are those of the participants and not those of BMO Global Asset Management, its affiliates, or subsidiaries.

Ben Jones - At the top of the episode you heard Paul Ewing, a senior technology consultant at Charles Schwab. I had the opportunity to attend IMPACT® 2017 and this year, like years past, the event did not disappoint. During the event I got the opportunity to sit down with four experts and have a round table discussion on cyber security as it relates to advisors and their firms.

Emily Larsen - It's an important and ever changing topic that requires systems, outside vendor relationships, and diligence. In addition to Paul, we were joined by Sten-Erik Hoidal, Sandy Smalley-Fleming, and Jake Omann. We'll let them introduce themselves to you now.

Sten Hoidal - Sten Hoidal, I'm a shareholder at the Frederickson and Byron Law Firm, which is about a 275 person law firm based out of Minneapolis, and at that firm I chair our firm's data protection and cyber security group.

Paul Ewing - Paul Ewing, I'm a senior technology consultant at Charles Schwab and Co, I work in the advisor services part of our business and my role is really to help advisors navigate technology decisions.

Sandy Smalley-Fleming - I'm Sandy Smalley-Fleming, I'm a shareholder at Frederickson and Byron. I co-chair our investment management and securities litigation group. I'm a securities litigator and on the defense side, so defend financial institutions, brokers and advisors when they're sued by their customers, when they get investigated by regulators, and I also provide advice to the same folks.

Jake Omann - Jake Omann, I'm with Associated Benefits and Risk Consulting. I'm a management liability consultant and I -- two roles really, one is leading our management liability practice which encompasses specialty insurance products such as cyber liability insurance, which is obviously what we're talking about today, and the other role is helping our clients with global risks and that could obviously relate to cyber as well as other just general global insurance risks.

Ben Jones - This episode is a first for the podcast and we hope we get it right. Four guests, one conversation, one episode. The conversation was pretty free-flowing discussion, so throughout the episode you may lose track of who's speaking about what. But we'll do our best to keep the guests identified for you throughout the show. Now that you know who our expert guests are, it's time that we level set what can be a very complicated topic, as I certainly learned during this discussion. After numerous highly publicized data breaches and hacks this year, the subject of cyber security has been heightened in all industries. Sten and Paul tackled level setting this topic for all of us and some of the common ways that breaches happen.

Sten Hoidal - I'd define it as the technologies, processes and practices that are designed to protect computer systems, networks, programs and data from unauthorized access, use, miss-use, theft or attack.

Paul Ewing - I tend to look at it from the RIA side of things and it's really more about technology and compliance and your policies and procedures that every firm should have as part of their own business strategy. Most of the time that we're seeing breaches or some sort of incident; it is generally generated around some sort of inbound e-mail. So e-mail contains a lot of bad stuff and really that's where I'm seeing it on the RIA side as far as employees clicking on links or invoices coming in that are fraudulent, and then also on the client side the end client side, their e-mails are being compromised and transactions are fraudulently being created by the fraudsters to gain access to those assets. The traditional sort of the breaking in from the outside, that penetration, I'm not seeing that too much in the RIA space, it's certainly out there and is certainly happening, but it's definitely on a lower side, I know Sten you have --

Sten Hoidal - I think unpatched servers and software tends to be a vulnerability as well that gets exploited.

Emily Larsen - Wow, I didn't even think of the fact that the end client's e-mail might be the source of the fraudulent trade. There are some standard frameworks developed to assist advisors and firms, both within our industry and outside to develop practices for protecting against and responding to hacks and breaches of security. First we hear from Sten and then Paul.

Sten Hoidal - So there are a number of cyber security frameworks. I think the most common and probably talked about -- I don't know Paul if you agree with this, is probably the National Institute for Standard and Technology's Framework for improving critical infrastructure cyber security, and that's the NIST framework is what people in the biz call it, and that's basically a set of operational best practices, and recommendations for improving cyber security at the organizational level.

Paul Ewing - So at Schwab we've chosen the NIST framework that Sten mentioned and we have built tools and have resources around the NIST cyber security framework, so they don't have to choose one, they can go to that one, it's definitely well adopted and well known. Many compliance professionals are familiar with NIST. You have your IT professionals are familiar with NIST, so that's the one I see most often and then again that's what Schwab has built their resources around as well.

Emily Larsen - Ben asked Sandy to walk us through the state of cyber security regulations as they're currently set up in the United States and what the SEC's recent review has shown.

Sandy Smalley-Fleming - As a basic backdrop, Reg S-P requires investment advisors to adopt written policies and procedures that address administrative technical and physical safeguards for the protection of customer records and information. Reg S-ID outlines the duties regarding the detection, prevention and mitigation of identity theft and the investment advisor's act, rule 20647, requires written compliance policies and procedure, requires review of the adequacy of those policies and procedures, requires testing of the effectiveness of those procedures. And I thought I would go through at least a little bit of SEC basic guidance and then we can talk some about what the SEC focus on right now.

Ben Jones - I think that makes a lot of sense, I would love to hear too I know there's some states that have started like putting their own regulations in place.

Sandy Smalley-Fleming - Yeah.

Ben Jones - How does an advisor keep track of all this?

Sandy Smalley-Fleming - Right, well New York and Colorado are really the two states on the forefront of regulating in this area, and it has caused some both anxiety and I think a bit of confusion. I think in the industry there is some grappling with -- because this is a complicated area, it tends to be intimidating for advisors and principals of firms. Would it not be best for us to come up with some overall standards? The comparison between New York and Colorado standards, I think folks are coming out, thinking that Colorado is not as onerous as New York. They are requiring, if you're an advisor practicing in Colorado, you need to follow their rules. They're requiring an annual risk assessment. Those risk assessments do not have to be conducted by third parties, so not as expensive. They're requiring secure e-mail including encryption and digital signatures for e-mails with PII.

Ben Jones - Did you catch that little acronym? PII, which stands for personally identifiable information, which we'll discuss in more detail a bit later, but this, will come up several times throughout the episode.

Sandy Smalley-Fleming They are requiring authentication of client e-mail instructions and employee access to electronic communication and disclosure to clients of the risks of utilization of electronic communication. So the big difference between Colorado and New York is that

Colorado does not have the requirement for the use of third party vendors and they did delete the breach notification requirement to the Colorado department, so I think an analysis of both what New York and Colorado are doing, like I said before, Colorado is not quite as onerous. If you're an advisor practicing in Colorado you've got to follow their requirements, if you are a broker/dealer purchasing securities in Colorado, you've got to follow their requirements. Now if you look -- it's helpful to examine those specific requirements in the context of what the federal law is requiring because the SEC is again making cyber security front and center of one of its high priority items, but I think the SEC since their exams have been fairly rigorous, I mean they have conducted what was titled cyber security 2 initiative, where it went through and examined 75 different firms, broker/dealer and advisors, specifically looking for what's the state of policies and procedures, how are they being implemented, what's the follow through, how are employees being trained, how are they identifying risks, what are they doing about those risks, and out of this recent review they just published sort of their observations, which I think for most advisors and broker/dealers to be helpful to go online, it's a real detailed analysis of what they found. So they focused on governance and risk assessment, access rights and controls, data loss prevention, vendor management, training employee including senior management and instant response. So I thought it would be also helpful to briefly discuss some of the positive observations, and also issues observed because I think an analysis of what they view as positive is that broker/dealers and not quite as much advisors, but they're getting there, are -- they understand, we need policies and procedures in place. We've got to train our employees; we have to have some sort of a plan in place to deal with risk. But I think what the SEC has found in terms of recommendations going forward is that there's got to be more actual implementation of these policies and procedures. So it's not just good enough to have procedures in place, you have to be exercising them, you've got to be testing them, you've got to be training all of your employees. It's not good enough to say we're doing annual periodic training for all of our employees; you've got to make sure that you are really doing periodic training.

Emily Larsen - Sten added to Sandy's description of regulations for cyber security.

Sten Hoidal - What Sandy was talking about with New York having very prescriptive requirements that impact registered investment advisors and Colorado having less prescriptive requirements impacting registered investment advisors, that's -- if you kind of look large over the legal landscape that concerns cyber security generally, that's very common. You have this kind of fracture where they're overlapping and there's questions about who's laws do you apply to. I think it's important for listeners to know that we don't have a centralized cyber security law in the United States; we don't have a centralized authority that is responsible for overseeing cyber security in the United States. Compare that to like EU member states where they do kind of a centralized data protection authority, and as a result of that what you get overall is a mix of federal regulation -- federal laws, state laws, federal regulation, state regulation, rules sprinkled in with some executive orders sprinkled in with some industry best practices and all of that informs what businesses have to do.

Ben Jones - Now that we have a high level understanding of the landscape, I asked Sten and Paul about how an advisor would begin the process of protecting against a potential breach. First you identify the risks through what's called a risk assessment process.

Sten Hoidal - When you're thinking about the risk, I mean it's important to note it's not just an IT risk, the companies that are doing this successfully are looking at it as an enterprise-wide risk, that involves various aspects of the business, not just the IT department.

Paul Ewing - So once you have the risk assessment completed; now you have a broad visibility into what is the risk for the firm. And so the challenge becomes there's going to be a ton of risks, and so the advisor needs to have a process for prioritizing and identifying those risks so they can begin to make changes and implement changes.

Sten Hoidal - Yeah, I agree, I think the next step is you have your risk assessment, you figured out what your risks are, now you've got to figure out your risk tolerance and you use those two things to inform the policies and the procedures that you're going to put in place because there may be vulnerabilities and risks that are in your mind relatively low, and therefore you don't want to put your time, effort and resources into them.

Ben Jones - As an advisor, you deal with investment risk tolerance for your clients almost daily, but in this case, risk tolerance or your enterprise risk tolerance is designed to help you focus your efforts on what you believe are the highest priorities for your firm. Now I asked Sten what are the different levels of information that an advisor should be concerned with and here comes that little acronym again.

Sten Hoidal - So when you think of levels of information, you think about them in a couple ways. One is that it's based on obligation, right. So there's certain types of information that you will either have a statutory or regulatory obligation in regards to, and chief among those is personally identifiable information, PII for short, but that typically is defined as a first name or initial with a last name, coupled with a Social Security number, an account number and pin, biometric data, things like that. That's one category of information that you pay attention to because you have -- in 48 of the 50 states a notification obligation relating to any sort of cyber security incident that impacts that data. But when I'm thinking about it at a broader level, I think you can focus on the obligations you have and the types of data that those relate to, but there are other obligations, you have obligations to customers through any contracts you have entered into with them that may have confidentiality components or they may be providing you sensitive information. But beyond that, it really comes down to data assets and sensitive data assets and that's how I look at it, what are the assets, your crown jewels, the sensitive data that you have in your possession that you really care about and how are you going to protect those. As you start identifying those you'll tear it out, here's the PII and you know that has a regulatory or a statutory component that affects it, maybe you have some PHI, protected health information, that's governed by HIPPA. I think it may be easier to think about it as sensitive data assets and what obligations might apply to those.

Emily Larsen - So what are the components that make for an effective cyber security risk plan. Paul tackled this question and then Sten adds on to it as well.

Paul Ewing - So you want to have a group in your firm that is responsible for cyber security, and this is not just the compliance officer, chief compliance officer is not taking on all of this responsibility. So it's good to include others within the firm and create a committee that is responsible for the risk assessment and then seeing the plan through to execution. It's the risk assessment, so having a thorough, repeatable risk assessment, that is key because really you can't assess where your risks are without having a formal process for understanding what those risks are, and that goes back to identifying those risks, so it's having an inventory, it's understanding who your risky vendors are, it's knowing where your data is, and this -- once you've identified the risks, now you can then begin to put protections in place to protect the data, protect the policy, and then a lot of times you have to create -- if there's not a technology component to a protection, it's how do we solve this with a compliance policy and procedure.

Sten Hoidal - And I'll add, there's not like a one size fits all information security program, I think it would be nice if there were, but unfortunately listeners there's not. When I'm thinking about it, I think about it in terms of functionality and this is borrowing from the NIST framework, I mean whatever your program is, it needs to do five things. It has to be able to identify the risks and the sources of risk relating to your data and cyber security, it has to protect against those risks through technical and non-technical measures. It has to be able to detect incidents, we want to be able to do that, don't want them coming in undetected, and you have to be able to respond to any incidents and then recover from those incidents. So those are kind of the five things that it needs to be able to do and then based on that -- there are I guess common components that I see, the policies and procedures that are informed by your risk assessment, I'm making sure you have the appropriate IT structures and systems in place, having an incident response plan, have a vendor management program and employee training, I mean those are common components of the program, but there are certainly others that will be added depending on your risk profile.

Emily Larsen - Beyond putting your cyber security team in place, one thing you can do to guard against the pitfalls of getting hacked is purchasing cyber breach insurance policies. We asked Jake Omann what the costs and considerations should be when it comes to this kind of insurance.

Jake Omann - So the cyber insurance availability has changed as dramatically as the risks and the legal landscape has changed in this area. So I sold my first cyber liability policy back in 2005 and we called it Internet liability back then, totally unrecognizable as a cyber policy would be today. So historically what cyber has covered is more of a third party risks, and by third party I mean lawsuits, litigation, defense, regulatory investigations, fines and penalties, so once a breach happens, that third party risk from an insurability perspective like balance sheet, protection for those advisors, which is still there today, but on a total breach cost perspective, that really only encompasses about 1/3 of the total cost, where 2/3 are actually on what we call a first party side, which means there's no lawsuit, but you have a breach and you're hiring computer forensics to determine how the breach happened, what data was compromised, engaging legal counsel, not on the defensive side, but more on the managing the 48 states and the SEC and all these various regulatory and statutory requirements that go along with it, PR, public relations, expenses, crisis managed expenses. According to the state that your customers are residing in, actually notifying them that the breach happened, so those related expenses, so all those first party expenses are newer component in the cyber world, and there's a bunch of other things too, I could go on and on, but it's very evolving, very dynamic, so to answer your question, simply yes, there's for sure coverage, but I want to stress more of the first party importance because those are the ones that are imminent and those are the ones technically that are more costly than the third party side.

Ben Jones - Yeah, so there's all these costs that an RIA might encounter should they have a breach. And you can get insurance to cover these things. Now I've got to imagine with all the news headlines, the cost of this insurance has to be rising by the minute, at least in mind, supply and demand. Tell me how much does it cost and what are some of the things contractually that an advisor should be looking for in those insurance contracts, having had an insurance license in my past, I do know the devil is in the details.

Jake Omann - Yeah, I do a lot of reading on a daily basis. So the cost component is definitely a consideration when we're talking to our clients and to your point about the supply and the demand dynamics, they're completely against what conventional wisdom would say based upon the frequency of breaches, and it's more of a function of pure supply and demand economics of

there is an overabundance of carriers that have an interest in supplying capacity for cyber insurance, just because they see the growth rate, so by 2020, total cyber premiums in the industry are expected to be almost $20B, as of today they're about $5B. Conversely, auto insurance premiums are going to decrease by roughly 75% by 2025, and mostly due to autonomous driving. So they see the writing on the wall and they see the opportunity, so there's a flooding of capacity in the marketplace which is driving down pricing. Now demand hasn't quite kept up with supply, but it is starting to creep up, so I think outside of financial institutions and healthcare, the pricing is very, very competitive. So to give you an estimate, I mean it would see pricing as low as $1,000 for what I would call a good, robust cyber liability program.

Ben Jones - Annually or monthly?

Jake Omann - Annually.

Ben Jones - Okay.

Jake Omann - Annually, yeah, but it all depends on things that we're talking about here. It depends on the size of your firm, how many records you have, how you're protecting those records, the controls, processes you have around your cyber security, so it definitely depends and I love to use the attorney words, it does depend. But I think that listeners would be shocked if they haven't already experienced how competitive the pricing is for this product, despite the fact that again, the prevalence and severity of these breaches continue to rise.

Ben Jones - And what are some of the clauses that need to be considered or thought through or requested.

Jake Omann - So when we look at cyber liability and we talked to clients, it's not just fill an application and we'll get you a quote and here's your quote.

Ben Jones - Draw your blood.

Jake Omann - Exactly, yeah, it's not as painful as it may seem, but it's an educational process. So when we go through the application process, it is somewhat of a quasi-risk assessment process, so they're asking questions and the questions are being driven by what they're seeing from a breach perspective, what's causing breaches? So they're asking about security protocols and when we go through our assessment in conjunction with the actual application they have to complete, it's uncommon for us not to notice deficiencies. So we'll focus on those and then we'll dovetail those with services that our firm provides, we have partnerships with Frederickson and Byron and other law firms as well that can provide, or, to your question earlier about what other resources come along with an insurance policy, carriers are starting to do a better job at offering pre-breach resources. So employee training modules, actually end-point security products that they will offer complimentary other products. They'll offer their own cyber risk assessments that a lot of times can supplant or at least provide what the SEC and other regulatory bodies are looking for. Because these are provided by third party vendors that they have contracted discounted pricing with. For an advisor, what I would look for is obviously you want that third party coverage component because regulatory is a big issue. FINRAs already been handing down significant fines and penalties, and not all their policies will include that regulatory component. So that one for sure. The other one I would focus on -- two in the first party side would be reputational damages and contingent business interruption, and so reputational really didn't exist until about two years ago, and that is lost revenue, let's say you have a breach and you have 1M records exposed, client records, and because of that breach, clients no longer will

do business with you, so they end their tenure ship of their relationship due to the fact they're no longer comfortable with you safe-guarding their information, so literally they will pull the business from you, you lose that existing revenue, that lost revenue is actually insurable now. Now there's obviously a forensics analysis that goes into it, you have substantiate that, this client left because of this, but that reputational damage piece is actually covered component now or can be.

Ben Jones - How do you tender a claim, because I can't imagine you can just call up and say yep, we were breached. How do you prove that, how do you tender a claim?

Jake Omann - So this is another evolving area and I'm going to give an attorney answer, it depends. So a good distinction to make here is between an incident and an actual breach, which most people don't understand the distinction and so what an incident is a compromise of confidentiality or availability of an information asset, right, so it could be a lost laptop, it could be that your system did get impacted with malware, so that's an incident, but a breach is an actual compromise or disclosure of PII, PHI, that private information. And so depending on if you have an incident on your hands or a breach, that will dictate what your response requirements are, statutory or regulatory and then conversely what you need to do from an insurance perspective. So what we recommend and where insurance carriers have gotten better at is developing these what they call a breach response team, so insurance carriers, good ones, have dedicated breach response teams that are made up privacy attorneys, or ex-privacy attorneys, security consultants, and they will field those 24 hour, 7 days a week phone calls saying this is what happened, what do we do next.

Ben Jones - Insurance can guard against losses that occur once a breach happens, but it's very important to guard against potential breaches before they happen. Now over the years I've heard that most breaches come from your employees, so I asked the group about this and how to effectively deal with the issue. Sten starts by giving context to the issue and the Paul gives some examples as a follow-up.

Ben Jones - I hear all the time that your employees are your weakest link when it comes to cyber security. Now I am an employee so I'm a weak link and have got a lot of employees that are also weak links apparently, but what does that really mean and could you give examples, you mentioned this incident Jake, and there's incidents and breaches, maybe you could give me some examples of why the employee is the weakest link and then just some best practices or tips on how an advisor should think about mitigating that.

Sten Hoidal - Let me start by putting some context around the employee issue. We live in a world where there are more people that have a mobile device than use toothbrushes. That's a fact, more people use mobile devices than toothbrushes. So highlights the interconnected nature of our world, and that goes down to employees. They are highly mobile and highly connected and they're subject to whim and caprice and misdeed just like anybody else and that's why you see things focused on employees so much because it tends to be successful, and when people say they're the weakest link, they really are the weakest link. They lose laptops, they respond to e-mails from the famed Nigerian prince who is cash poor but has a great opportunity for you. That appeals to the emotion of employees. And so I think it's absolute, and those are just two examples, but it's absolutely true they're the weakest link.

Paul Ewing - We have a colleague of mine at Schwab who as we've been in the field for the past year and a half or so talking about cyber security, that individual on my team has been keeping track of how many incidents of ransomware he's come across. So I was with him just a

few weeks ago and that number now is over 50, so over 50 firms in the past year and a half that this one technology consultant has been talking to and interfacing with has had some level of a ransomware attack. So one of those firms was a successful attack, meaning that they had no backup systems, so they were needing to pay the ransom to release their data, and they did that, using bitcoin. So that's one example of a firm that needed to pay the ransom. So ransomware attacks are pretty prevalent, and again, that goes back to training.

Ben Jones - So employees are the weakest link because of the physical devices that they carry, but also the intrinsic emotional responses we have in general as humans. Sten gives one other example.

Sten Hoidal - A spoof e-mail was sent usually from the CEO of the company that said can you please forward me a PDF of all employees W-2s, and it would make its way into the human resources department or wherever and it worked like a charm because people, oh the CEO should be entitled to have the W-2s, no one ever thinking about why does the CEO need 18,000 employee's W-2s, and that's when we talk about training, that's the kind of awareness that you need to be generating among your employees, this idea that they're kind of vested in the idea of generating a culture of security at the company, because those are the -- that should be a red flag and there should be a call there to verify do you really want 18,000 W-2s, how is that helpful to you and why as the CEO would you need that information.

Emily Larsen - Unfortunately there may be as many as 15% of family offices that got breached this year, so in some sense it's about planning for when it happens, not if it happens. Our final area of discussion is a look at client relationships, how do you effectively communicate with your clients before and after a breach.

Jake Omann - Well it does go back to having your documentation in your incident response plan. So for an advisor thinking about your business continuity and disaster recovery plan, advisors are very familiar with those plans. The incident response plan, which we've been discussing, is something that needs to be well documented and needs to contain different scenarios of breach or incident. In that documentation you want to document who is going to be responsible for communication, and so a lot of times a firm will rely on third party PR resources there to help craft messages, but communication internally within the organization is very important because what you don't want to have is any sort of misinformation or miscommunication spread through internal communications as well as then those individuals talking to clients, so being very methodical and organized around just the message that you're going to convey to your clients is very important. It can be a third party that can help them with that messaging, but I think a lot of it just goes back to, since this is a trust and relationship business that we're in, is being honest and forthright with your clients and this also is where it's important to be up front with your clients before breach. So having those discussions with clients and I always tell advisors you want to try to monetize as much as you can with the efforts that are going into cyber security because you as a firm need to be able to communicate with those clients, hey this is what we're doing for you, this is how we're thinking about your data, this is what we're doing to protect that data, and pre-breach it's very important to monetize as much as you can with that information, and that can be just one-on-one discussions in meetings, it could messaging through your website, it could be monthly or quarterly communications that you have with your client and I'm always impressed with firms that include some sort of tips and tricks around cyber security for the end client because as we've been talking about, employees are a big risk, well your end clients are just as well a risk that you need to be thinking about, and so the more effort you can put into -- not so much marketing to those end clients, but at least communicating with them on the importance of cash management and updating their systems

and all the things that we've been talking about don't click on links and call to verify instructions, don't rely on e-mail communication.

Emily Larsen - I really like the idea of providing cyber security tips to your clients on an ongoing basis, so if or when something happens, it's not the first time they've heard about the subject from you. We've covered a lot of ground today. We've discussed defining risk through a risk assessment, setting up a committee, protecting yourself with systems and insurance, training employees, we've also talked through some examples of real breaches and how to communicate with the end client. Here's how Paul and Jake summed up our conversation in a few words.

Jake Omann - You need to be prepared for cyber security and it's not going away.

Paul Ewing - What we're talking about today only is relevant today, so in other words you need to stay abreast of these changes because what we're saying today may not be relevant even tomorrow or next week.

Ben Jones - As Jake mentions, this is an ever changing topic, and to help you stay relevant and abreast of the changes, we've compiled a list of tools and resources from our expert guests. You can find those at bmogam.com/betterconversations in the show notes sections. Now all of our guests offered to discuss this topic with our listeners and freely offered up their contact information, which you can also find in the show notes as well. We are deeply grateful for the time and expertise that our panel of guests provided us for this episode. Thank you so much Sten, Paul, Sandy and Jake.

Emily Larsen - We also want to thank Robin Gibson and Bret Solnoki for making this episode possible.

Ben Jones - Thanks for listing to *Better conversations. Better outcomes*. This podcast is presented by BMO Global Asset Management. To learn more about what BMO can do for you, visit us at www.bmogam.com/betterconversations.

Emily Larsen - We value listener feedback and would love to hear about what you have thought about today's episode. Or, if you're willing to share your own experiences or insights related to today's topic, please e-mail us at betterconversations@bmo.com. And of course, the greatest compliment of all is if you tell your friends and co-workers to subscribe to the show. You can subscribe to our show on iTunes, Google Play, the Stitcher app, or your favorite podcast platform. Until next time, I'm Emily Larsen.

Ben Jones - And I'm Ben Jones. From all of us at BMO Global Asset Management hoping you have a productive and wonderful week.

Emily Larsen - This show is supported by a talented team of dedicated professionals at BMO, including Pat Bordak, Gayle Gipson and Matt Perry. The show is edited and produced by the team at Freedom Podcasting, specifically Jonah Geil-Neufeld and Annie Fassler.

Disclosure - The views expressed here are those of the participants and not those of BMO Global Asset Management, its affiliates, or subsidiaries. This is not intended to serve as a complete analysis of every material fact regarding any company, industry, or security. This presentation may contain forward-looking statements. Investors are cautioned not to place undue reliance on such statements, as actual results could vary. This presentation is for general

information purposes only and does not constitute investment advice and is not intended as an endorsement of any specific investment product or service. Individual investors should consult with an investment professional about their personal situation. Past performance is not indicative of future results. BMO Asset Management Corp is the investment advisor to the BMO funds. BMO Investment Distributors LLC is the distributor. Member FINRA/SIPC. BMO Asset Management Corp and BMO Investment Distributors are affiliated companies. Further information can be found at www.bmo.com.

C11: 6382538