Market Update Call – Audio Transcript
November 18, 2015

Speakers:

John M. De Clue, CFA
Chief Investment Officer
The Private Client Reserve

Jason Witty
Chief Information Security Officer
U.S. Bancorp

Opening: This is a recording of the U.S. Bank Wealth Management Market Update Call held on November 18, 2015. The discussion featured insights about the increasing frequency and severity of cyber attacks, the evolving nature of cybersecurity, and how deeper awareness of the problem may lead to better protection and solutions.


Given the tragic events in Paris last week, security is, I'm sure, on everyone's mind, and I will make some brief comments about these events and what they may mean for investors at the end of our call today. But it's not only our physical security that's on everyone's minds but cybersecurity as well, and this is the focus of our discussion today.

This past January, in fact, we held a national call on this very topic, but cybersecurity continues to evolve and as the frequency and severity of cyber attacks increases, we need an even deeper awareness of the problem in order to craft better solutions.

Investment products and services are:

<table>
<thead>
<tr>
<th>NOT A DEPOSIT</th>
<th>NOT FDIC INSURED</th>
<th>MAY LOSE VALUE</th>
<th>NOT BANK GUARANTEED</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOT INSURED BY ANY FEDERAL GOVERNMENT AGENCY</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
As was the case in January, joining me today, therefore, is Jason Witty. Jason is chief investment security officer with U.S. Bancorp. He's a frequent speaker on the topic of cybersecurity and has received national recognition for his work in the security information industry.

Thank you once again, Jason, for joining us today.

Jason Witty: Thanks very much for having me, John.

John De Clue: Thinking back to January, can you give us a sense of how dramatically the Internet and Internet usages have changed between then and now?

Jason Witty: Absolutely. The Internet has been growing explosively for approximately the past ten years, and most people would understand that. But if you just look at what's happened this year, as Americans, a lot of Americans will tend to think of the Internet as an American thing, and 20 years ago that was really true. But what we've seen over the past 12 months, 18 months, 36 months is the entire world is now connected together.

If you look at the broad numbers of people that are actually connected to the Internet, that growth went from about 2.8 billion last year to about 3.5 billion. Now, put that into context, we've got about 7 billion on our planet, we literally now, this year, have about half of the world's population directly connected to the Internet.

What's really interesting about that number though is it's not just people connected to the Internet anymore, its things and lots of things. So in that same planet where we have 7 billion people, we have almost 2.5 times as many things connected to the Internet. Whether that's airplanes and you're getting your Gogo Wi-Fi access on your flight or your car that's phoning out to the Internet in order to get weather patterns or driving instructions, or whether it's your watch or your pedometer or your pacemaker, for that matter. We're starting to connect more and more and more things to the Internet, and that's resulted in an Internet population of approximately 18 billion to 20 billion things by the end of this year.

John De Clue: It seems like cyber breeches and attacks occur at companies and government agencies now almost on a daily basis frankly. Give us a sense of how the cyber threat environment has changed.

Jason Witty: So it's really interesting to consider how dramatic things are and how fast things are accelerating. There's a concept in information technology called Moore's law that says that the rate of technology change will double every 18 months. We've been seeing that ever since the Internet was born when it was just a few people.

Now we've got half the world's population on the Internet in 2015. Same thing holds with storage. The amount of data that we have, even in our personal lives, tends to double. Who deletes all of their home email, right? You typically will have a lot more data.
Companies have more and more data. We have a lot more speed, higher speed connectivity. A lot of these things are facilitating very good growth and a sort of emerging digital economy, but at the same time, the threat environment has been changing with that same sort of pace.

If you look at the number of different types of threat actor that exists on the Internet, you've got to consider pretty much five areas. One is insiders, which don't happen that often, but when an insider at a company decides to do something really bad, typically they'll have a lot of access within that company and they're able to do a lot of really bad things with that.

So although it's not rare it's not super common. When Snowden happens, for example, to one of the arguably most secure organizations on our planet, the National Security Agency (NSA) of the United States, that was a really, really big deal. So that's one of five.

The second that anyone attached to the Internet, in one way shape or form, is dealing with organized criminals. And organized crime has been growing explosively over the past 18 months, fueled by a lot of very successful breeches, a lot of very successful data and data thefts, data for sale, big data mining services.

This has become a full time job for organized crime multiple years ago, probably seven or eight years ago now, and it's become such a mature industry with billions of dollar in funding that they can have full-time help desks, they can have full-time virus writers, they can have Q/A teams that are making sure that the viruses aren't detected by commercial antivirus software. There's a lot that comes with having billions of dollars in funding.

Then we have hacktivism, which is a new thing powered by social media, new thing as of about three or four years ago, but this year has really been shifting from not just well intentioned or people that have some sort of ideological problem with a company or a country and want to do something from an activist standpoint online, which was the way that would have typically shaken out two or three years ago. Now we're actually seeing that morph into a fourth category, which would actually be real terrorism online.

So imagine that there was news reports, the tragic events last Friday, it was very clear that some of the terrorist groups are in control of tens of thousands of Twitter accounts, use those for recruiting, use those for propaganda, use those for terrorizing people, putting up images, blasting that out all over the Internet.

But there's a very growing sort of bleed over between traditional hacktivism that social media engaged and can get tens of thousands of people to go do something and now terrorists, using the exact same type of capability, maybe at a higher level of encryption that's harder to actually detect if it's operational in nature, for example.
And then we have the fifth category that's really interesting. And by the way, I should probably pause at this point and say all of this is meant to educate you, not to scare you. I always forget to mention that at the outset. Now that that's said, the fifth area that's really interesting and has exploded over the past 12 to 18 months is nation state activity.

Between the years of 2008 and 2014, U.S. Bank was tracking approximately 18 cases of in the news, publicly citable cases where countries had used cyber weapons against companies, or countries had used cyber weapons against other countries. So there's a lot of examples of that.

In the past calendar year for summarizing 2014, there was a report that came out in March of this year that says that there were 56 documented cases of that happening in the 2014 calendar year alone. So there really has been this awakening that's happened where countries are realizing that they can use cyber as a military vehicle just like they would use air, sea, land, space, et cetera. And this is an emerging field that we all need to be thinking through, especially as we go into the new administration and the focus that the administration has currently has had in cyber, and what the transition is going to look like to a new presidency in the United States. That's going to be a pretty big deal.

John De Clue: Eluding back to the tragic events in Paris. There's discussion in the press about intelligence agencies and cooperation between them, or sometimes the lack thereof, I guess. When it comes to cybersecurity, what is international law enforcement doing to confront the threat in different regards?

Jason Witty: So I'm going to first start by saying that law enforcement has a very tough job. The reason for that is the legal landscape on the Internet is far behind the technology innovation that has happened on the Internet. It's also far behind the kind of criteria for a country coming onto the Internet.

There is no criteria that you have to abide by as a country in order to join the Internet. And so put simply, it's not illegal to hack from many of the countries that are connected to the Internet. In some cases, it's not illegal to steal money from the Internet, from Internet users and bring it into that country.

Where it is illegal, there are even cases where it's illegal within the country, but if you pull it outside of the country, it's not or if you execute it outside of the country and came back, then you're fine. So a lot of just complexities that come with global law enforcement in general.

That being said, law enforcement has really upped its game in the cyber realm over the past three to four years. This year alone there's been a couple of very unprecedented things. When the Obama administration declared a national emergency for cybersecurity in our country on April 1 of this year, law enforcement really took that to heart.

One of the things that they did is up the game relative to going after criminals and prosecution. The Department of Justice in the United States basically
raised some of the prosecution minimums and is trying to have harsher sentences and treat this less like white collar crime and more like, hey you just robbed a million people using your computer and that's a big deal.

So for the first time ever, we have an FBI reward for a cybercriminal this year. It's a guy name Bogachev, who was responsible for the GameOver Zeus malware that has been circulating the Internet. It's estimated it stole $100 million, and he profited from that himself. So one individual, $100 million. They're offering a $3 million reward for his capture.

Now that sounds like a lot of money, and it absolutely is a lot of money. What's really interesting about that is the context though. When the FBI puts out a reward, typically a hard-to-catch murderer will go for $150,000 or $250,000 reward. So for them to put $3 million on one person's head from a cyber perspective is a really, really, big deal.

There's also simultaneous effort by the administration to aid law enforcement that has come by way of several executive orders that have been released. But it's really trying to make other instruments of national power outside of law enforcement a deterrent to cybercrime.

So what I mean by that is, we are now starting to use sanctions, for example, against individuals, against teams, against companies or countries who are declared by law enforcement as having done some sort of hacking or theft or intellectual property theft, whatever it is, against a U.S. company, and specifically if that company is designated as critical infrastructure at the United States then this for sure would apply.

But we now have a treasury vehicle for doing that, and that is something that's unprecedented. It just started happening as of this April 1 declaration of emergency in cybersecurity and the executive order that came with that.

John De Clue: Interesting. You talked earlier about one of the five angles, if you want to call it that, organized crime being one and then state involvement, corporate involvement. So I'm guessing there's a lot of money on both side of the equation here. What is the financing look like on the attacking side of the equation and then on the other defensive side, I guess those that are trying to protect themselves?

Jason Witty: So it's really interesting to consider cybersecurity projects, products, services and technology as a market in general. That market has been growing for the past three to five years, depending on your measurement, somewhere between 7 percent and 8 percent compounded annual growth rate. By the end of this year, it's estimated by Gartner that that will be a $77 billion industry that very likely, over the next three to five years will reach somewhere around $130 to $140 billion industry.

This is definitely a space to watch carefully as the Internet matures and as these types of attacks continue and as the technology footprint starts doubling,
right? What we're seeing now is going to be dramatically different than what we see in 18 months. Watch this space on the spending side.

On the cost side, this is where it gets really interesting. Part of the cost of information security, or breaches, or fraud, or all of these other things, if you add all of that up together, there is a conservative estimate that was put out by an antivirus vendor, McAfee, but very conservative effort, they tried to put as much data science behind this as they can. They had several partners from universities review the numbers and the math behind it, and they feel very comfortable in saying that the attacking side, the cost of all of this stuff to the global economy, is $575 billion. So on the defensive side, we're spending $77 billion; the cost to the world economy is $575 billion. Again we're talking about a highly, highly well-funded adversarial environment.

Some of you may have heard of the business e-mail compromise scheme that's going around. And it basically – somebody purports to be your CEO and they send in an e-mail to your CFO or your controller, get them to think that there's an acquisition deal going on that needs to be funded in China or some random variant of that. And then the CFO thinks it really was the CEO, doesn't call them, doesn't validate it in person, doesn't have any other validation, puts it through, thinking it was them, and then they've lost the money.

Well that particular scam by itself is a handful, probably estimated to be somewhere around 20 to 25 people who are really social media savvy, who know how to use social media to get the org charts out of companies, and have actually themselves, by this one simple tricking, spoofing e-mail scam, they have pulled out over the past 12 months $1.3 billion from the world economy.

John De Clue: Wow. Unbelievable.

So, Jason, it's likely that a number of listeners to this call own businesses, run businesses or do both. What advice would you give companies, what should companies be doing to protect themselves?

Jason Witty: I could talk all day long about specific nuances and business models and that sort of thing, but there's a very small number of things that are very common that successful security programs have. The first is there is an accountable person for information security. It doesn't really matter if that person carries the title of chief information security officer or director of information security, or for that matter they're actually the chief technology officer and they also are designated by their CEO as being accountable for information security for the company.

But the key point is, the first thing is, you have to have somebody at your company who is accountable for information security and if things go wrong. The second is picking a framework for information security controls that you can roll out at your company. And that could be a very robust one if you're a very large company and you're in lots of countries and you need to think through a lot of different regulatory factors or that sort of thing.
Or, it could be very simple. You're a donut manufacturer and you've only got one kitchen and you're doing that every morning and you've got some POS (Point of Sale) terminals you need to worry about because you're accepting payment cards and that's flowing through your network, that can be very robust or very simple.

There is a framework that came out last year that's been adopted widely this year called the NIST (National Institute of Standards and Technology) cybersecurity framework. That one is certainly something that allows you to maturity rank yourself on about 98 different types of areas that if you did most of those you'd have a reasonable control set.

The third thing I would say is put really large focus on e-mail, what's going out in e-mail, what's coming in in e-mail. U.S. Bank, just as an example, we typically block somewhere around 90 percent to 95 percent of what's actually attempted to be delivered to our employees.

John De Clue: Really?

Jason Witty: That's because – really. It's because there's that much that's coming in from this sort of bad neighborhood we call the Internet that is scams, its spam, sometimes its marketing or advertisements, but a lot of times its viruses, it's spoofing, it's a lot of different stuff that we just don't want in our employees' inboxes.

That by itself helps us keep a lot of badness from happening, but I can't stress enough the focus on training employees not to click on things in e-mail, being really super careful with attachments in e-mail. Again, we got 3.5 billion people connected to each other in this bad neighborhood we call the Internet, and there's no concept of distance.

So with a real world scenario, you've got an organized crime boss and there's a bad neighborhood and there's a good neighborhood and you just stay out of the bad neighborhood. Well everybody connected to the Internet is connected to this sort of bad neighborhood and anybody can send anybody else e-mail. So you've got to be really, really careful with how you use e-mail, what you're putting in it and the sophistication that you're applying to monitoring what's going in and out.

The last thing that I would just say in that is computers do not stay secure over time. Quite literally, if you have a secure computer or device for that matter, it could be your phone, your iPad, whatever, if you had it secure and everything's up to date and you turned it off and you stuck it in the closet for 30 days and you come back, that is now an insecure computer that if you connect to the Internet, it could be hacked.

And the reason for that is you're 30 days behind 70,000 new virus signatures that come out every single day, you're behind multiple critical Java patches that have been released to the Internet fixing some kind of hole that could allow somebody to exploit your system without even having a user ID and
password, or you're exposing yourself to operating system vulnerabilities that will have then patched in the monthly patch cycle.

Whatever it is, there's a lot of different criminals that are banging away at software looking for holes, and every month there are hundreds of things that vendors publish as new updates that need to be applied in order to keep those systems secure.

John De Clue: Let's turn to the individual now, what individuals can do to protect their home networks. And as a matter of fact, thinking back to January, you made one suggestion that I actually in my house implemented. Talk to us about what we, as individuals, ought to be doing at home to protect ourselves.

Jason Witty: That same hygiene that I mentioned on the corporate side, also think about at home. That's rule one, things like patch management, making sure that you have automatic updates applied, that you've got an antivirus product of some kind, you're updating that once or twice per day, automatically. It's not that you're doing it, right, but you set your system to automatically download these things, apply them. You want to do that sort of basic hygiene.

The second is the exact same rule that applies for corporations: be super careful in e-mail. If somebody sends you something that is overly urgent, it's probably a scam. If someone sends you an attachment that you weren't expecting, it's probably a scam.

I'll give a couple of examples of that, just quickly, that are going around right now. One of them is looking for people who have some sort of manager title in their online profile, so LinkedIn, Bebo, what have you. Then knowing that they're a manager, sending them something to their personal address, whatever the address was that you used on LinkedIn, I'll use as an example, and then they say that they're an applicant and would be interested in applying for a job and they send you a PDF document that has a virus in it that you have no idea about.

And as soon as you think, "Oh that's interesting, I might actually be hiring somebody soon." Then you open the attachment. Now you've got that on your home computer. Now it's recording everything that you're doing. It's sending those keystrokes somewhere else, and it could allow them access to your home life for sure, but depending on what you're doing for work off of that device or what you're typing in for work in order to do your daily work maybe on that device, then that could be compromising that information as well.

So the same thing that applies to corporate applies to personal. Be really careful about what you're clicking on in e-mail.

The other thing I would say about home users is, there's a lot social kind of dos and don'ts. The number one that I would just say is regardless of what sort of social media policy you have at home, you want to have some kind of social media policy with your family. For me, I have little children. They're 11, 9, and 4. So I tell my kids that the only place you're allowed to lie is the
Internet and you should expect that other people are not being truthful about who they are either.

That one simple rule for us makes them a little bit more suspect when they think they're talking to an 11-year-old girl in a chat room. It's a little different, right? You might not actually think that what they're saying makes sense in that context, or those types of things.

There's also a lot more that can go into a social media policy around what are you going to post online, do you ever want to allow your home address to be posted, your school's name, any of those types of things. You probably want to think through some of that as an individual and what's appropriate for your family, what's appropriate for your children, maybe your grandparents for that matter.

But one thing I can say with certainty is you want to be very, very careful with location services. More and more apps, there's this sort of app for that phenomenon that's going on, more and more apps are location aware or could be location aware if you grant that app the access to your current location. And that's great if you're using the phone's map app and you need to get to a certain location and it needs to know where you're at in order to calculate where you're going. That's fine.

But why does a game app like Angry Birds or something need to know your location? So you need to be very deliberate with location services, especially deliberate about posting any sort of vacation photos or "hey I'm going to this party tomorrow night at 8 p.m. at this particular location" because that immediately tells the bad guys that you're not going to be home or that you are going to be in some other place, and that can open you up as a home user for a lot of badness.

John De Clue: Interesting. And the recommendation you made to me that was very practical for me, and I know may not be for others is to set up a sterile computer, I think you called it, at home. I just so happened to have upgraded, didn't know what to do with my old computer, and effectively now use that computer for only business and personal financial stuff, if you will, and never connect to e-mail through it.

How often do programs like McAfee and Norton, take your example of a PDF with a virus embedded, the applicant, are they able to pick that up or not always?

Jason Witty: Let me answer the first part on the devices first. The average, kind of okay computer, right now has come down in cost to somewhere around $300 to $400, so it's actually quite economical these days to be able to have a brand new computer that you do absolutely nothing else with other than you use it for your bills, you use it for your finances, you it use for your online purchases, et cetera, and you just do that. You don't read e-mail on it, you don't generally surf the web on it.
You can even take a tablet device like an iPad or something like that and use it for the exact same purpose. So don't e-mail, don't do browsing, but you do all your, you know, main shopping and your bank and that sort of thing. And that is a very, very safe way of kind of eliminating the e-mail borne threats and the "hey I accidentally clicked on a link that I really shouldn't have in a Google search" or something that now blasted down one of these viruses.

The reason why that's so important is the root of your second question. There are 70,000 new viruses on the Internet every single day. It takes the commercial antivirus vendors somewhere between 24 to 48 hours to find them, create a detection routine for them, publish those signatures out, and then make that publicly available for production application.

So again, the attacker has got somewhere between a 24- to 48-hour window where this is going to be pretty effective and the more people you can get it out to, the more people click on it, the more badness the virus is able to do. That's the reason why you want to update your signatures multiple times per day but still know the antivirus isn't going to stop everything and be very careful with where you're browsing and what you're doing in e-mail.

John De Clue: I got it. Let me conclude with talking about the aging population, and I'm part of it as a Baby Boomer. I was thinking about this the other day. It was my mom's birthday. I've lost both my parents because, you know, I'm well on in age personally. But nevertheless, I was thinking about something. They never, either one I don't believe, ever touched a personal computer, whereas I, you know, was starting to use a PC shortly after IBM came on to the market in '82, '83, '84, somewhere in that range.

So I, like others in my generation, are completely computer savvy, if you will, and moving in to the latter chapters of our life. Talk to us about the advice you might have for us, any of us trying to help elderly parents or grandparents from becoming victims, very frankly.

Jason Witty: Unfortunately there's a growing trend towards targeting elderly individuals specifically. And the reason for that is, typically that generation tends to be very helpful, tends to be relatively trusting, tends not to be technically savvy, and also at the same time tends to have money, so some kind of life savings, 401(k), whatever it is. So those four factors add up really quick to, "Hey this is a really good victim" from an attacker's standpoint.

One of the most common scams that go around these days is a phone call comes in and they say they're from, say, a large tech company and you've got a virus on your computer and…

John De Clue: Oh yes, I've gotten them.

Jason Witty: ...financial information. Absolutely. My mom got one. And, you know, we need to log in to your computer immediately in order to get this virus off your system. And what they wind up doing is talking you into installing a remote
access Trojan that then allows them full-time access whenever they want to
your system.

It also winds up giving them administrator rights so now they can basically
copy off without your knowledge, copy off your data, all your files, all of that
sort of thing, and then of course they can record whatever keystrokes you're
putting in from that point forward, including whatever you type in your bank,
whatever you're typing in to your healthcare company, et cetera. That's a
really common one.

Another one is just simply the exact same thing I said for home users in
general needs to be reiterated to the elderly population, and that's being super
careful in e-mail. I kind of joked a few years ago with my mom, when you see
that thing that pops up that says Okay or Cancel, it's okay to say cancel. You
don't have to say okay.

And that does trick a lot of people, right? If there's a virus that pops up and
says I'm going to take all your bank account information okay or cancel, you
just click okay. It's okay to say cancel. So that is one of those other big areas.

The third one that I would kind of cite for anyone but especially for children
and for the elderly is credit monitoring. A lot of companies are offering,
because they got breached and your personal data was lost, free credit
monitoring. You can also pay for credit monitoring. I have a service that I use
that monitors my family.

But the interesting thing is on the child side of it, if an adult's credit is taken
over by someone else, so you've had identity theft, you'll typically notice that
within a 60 to 90-day window. If a child's identity is stolen, they might not
notice until they're 18. So if you hit them when they're 15, 16, that's a really
good target because you might actually own that identity for three or four
years. So that's on the child side.

On the elderly side, it's very similar. You've got a lot of credit, you've
established a lifetime of savings, you've established all these things, you want
to get some sort of monitoring service that you're not applying for new stuff
that you didn't expect or that you didn't just draw down your credit line all of
sudden that you weren't expecting. There's a lot of services out there that can
just watch your social security number, watch your maiden name, whatever it
is, and just make sure that that's not causing your credit file some sort of issue.

John De Clue: Well that's interesting. And I have not heard about that before but I'm
certainly going to check it out as I did back in January with the idea of a
separate sterile computer.

Well, Jason, that brings us to the end of our discussion. And once again I can't
thank you enough for taking the time to speak with us today. Unfortunately I
have a feeling we're going to have a regular stream of these conversations
with our clients and prospective clients, but better that than we all be aware
and forewarned and armed against this threat. So again, Jason, thank you so much for joining us.

I would guess that during our discussion, some of our listeners are asking themselves are there investment opportunities in the space of cybersecurity. And of course there are.

In fact back in January, our Strategic Equity Group under our chief equity strategist put together a basket of stocks representing companies that are engaged in this industry. And we provided this list back then to our investment professionals. We're in the process of updating that list and pushing it out again, and we should have a new set of opportunities available in a week or so. And I would ask you contact your U.S. Bank advisor for further information.

As we expected, you want to be diversified in this space. As we look back as to some of the stocks we've been tracking now for, you know, 11 months or so, some have done very, very well, some have not. So, diversification is extremely important in this space.

So let me bring the call to a close, but as I said at the beginning of the call, I'd like to make a few brief comments on the terrible events in Paris last week as they relate in general to the subject of terrorism and the investment markets and how concerned we should be about them.

In fact we've just published a situation analysis paper on this subject, which your U.S. Bank advisor would be happy to share with you, so please ask if you have an interest in reading this paper. It's much more detailed than the following brief comments.

So in a nutshell, looking at past terrorist incidents, however horrific in terms of intent, and I mean evil intent and loss of life, the impact on investment markets generally has been relatively short lived. In fact, although key stock exchanges in Europe and the United States did sell off somewhat following the recent Paris attacks, those pullbacks ranged from down 1.1 percent here in the United States in terms of the S&P 500 to about 1.8 percent in the case of the French CAC Quarante 40. And again those are significant declines but not huge declines.

The interesting thing is, as I speak to you now today, this index, the CAC Quarante 40, in French as well as the German DAX and the S&P 500 are all trading from 1 percent to 1.75 percent above their levels immediately before the attacks. Tragically looking back, there are all too many incidents to examine such as a spate of attacks in the 1970s and more recently of course 9/11, the 2004 Madrid train bombings, the July 7 London attack.

And in most of these cases, the long-term impact has been more political or social than economic. I'm not trying to suggest though we should be complacent. If the Paris attacks are not a one and done one-off thing but the beginning of a regular series of atrocities like this, things could be different.
Europe is particularly vulnerable, I suppose, both from a political and an economic point of view. Economically, any fall off in consumer spending – and think about the impact on tourism, Air France for example and some hotel chains in Europe are sharply down, their stocks are sharply down after these attacks – any fall off in consumer spending, especially tourism, is likely to hurt growth, which is already barely evident in Europe.

Politically as well, the attacks in Paris have put a great strain on issues such as free travel between European countries, the treatment of Syrian refugees, the rise of Euro-skeptic political parties in Europe, as well as weakening unquestionably the most powerful leader in Europe, Angela Merkel of Germany. She has taken a very liberal stance on the refugee situation, as you know, and now is under fire.

But these events will take time to unfold. I did want to make the point though, however awkward, that looking at history, terrorism, however horrific, does not seemed to have a major impact on the financial markets to date. We just should hope that that doesn't change.

As I wrap up today's conversation, thank you very much for your relationship with U.S. Bank. And again, please contact your U.S. Bank advisor if you have any questions about the call.

**Closing:** Thank you for listening. We invite you to join us for future calls. Details can be obtained from your U.S. Bank representative.

Website: reserve.usbank.com

The information shared by the speakers represents the opinions of U.S. Bank and does not constitute investment advice and is issued without regard to specific investment objectives or the financial situation of any particular individual. Since economic and market conditions change frequently, there can be no assurance that the trends described will continue or that the forecasts will come to pass. These views will be valid as of the date presented and are subject to change at any time based upon market or other conditions. The information presented is for discussion purposes only and is not intended to serve as a recommendation or solicitation for the purchase or sale of any type of security.

Based on our strategic approach to creating diversified portfolios, guidelines are in place concerning the construction of portfolios and how investments should be allocated to specific asset classes based on client goals, objectives and tolerance for risk. Not all recommended asset classes will be suitable for every portfolio. Diversification and strategic asset allocation do not assure profit or protect against loss in declining markets.

**MARKET UPDATE CALL TRANSCRIPT – November 18, 2015**

Important disclosures provided on page 13.
The **French CAC Quarante 40** is the French stock market index which tracks the 40 largest French stocks based on market capitalization on the Paris Bourse stock exchange. The **S&P 500 Index** is an unmanaged, capitalization-weighted index of 500 widely traded stocks that are considered to represent the performance of the U.S. stock market in general. The **German DAX Index** includes 30 of the largest and most liquid German companies that trade on the Frankfurt exchange.

**Equity securities** are subject to stock market fluctuations that occur in response to economic and business developments. **International investing** involves special risks, including foreign taxation, currency risks, risks associated with possible difference in financial standards and other risks associated with future political and economic developments. Investing in **emerging markets** may involve greater risks than investing in more developed countries. In addition, concentration of investments in a single region may result in greater volatility.