Fidelity Viewpoints®: Market Sense

Week 73, October 19, 2021

TRANSCRIPT

SPEAKERS:

Jim Armstrong   Jurrien Timmer   Leanna Devinney

Jim Armstrong: Hello and welcome to Market Sense. Thanks for joining us. I'm Jim Armstrong with Fidelity.

On this show we tend to talk a lot about risk, how to reduce your risk in your portfolio through diversification, for example, lately we've been talking about the risks of inflation. Well, today in recognition of the fact that October is Cybersecurity Awareness Month, we thought we'd talk about a different type of risk related to cybercrime. Certainly it's something that is on all of our radars, something we probably should all be thinking a little bit more about, and maybe even come up with some ways to protect ourselves from it if possible.

So, that's what we're going to be talking about today. And to have that conversation we're joined by Fidelity's Jurrien Timmer as always. He's going to give us a glimpse into the latest market news and developments.

And then Leanna Devinney is here as well and in addition to her analysis, she's going to provide some practical steps that can help us all ideally, hopefully, keep our money a little bit safer. So, Leanna and Jurrien, thanks for making time again to be with us this week.

Leanna Devinney: Thank you so much. It's great to be here.

Jurrien Timmer: Great to see you guys.

JIM: So, Jurrien, it is Tuesday, October 19th. And I thought maybe we could start off with just a high level look at the markets as we ease, whether we like it or not, into late autumn at this point.

You know, one metric we haven't looked at in a while is COVID cases and their impact on the economy and the market. So, maybe start there.

JURRIEN: Yeah. And there are certainly some good news to report, you know, on this chart. I've shown this in the past.

I've looked at the number of hospital beds in the US occupied by COVID patients and so that's a good barometer of what the impact of the pandemic is on—obviously on people and by extension, the economy. And you can see here that that Delta wave really has come down very nicely. You know, we went from 2% of hospital beds being occupied by COVID patients up to 14% and we're now down to 8%. So, clearly the Delta variant wave in the US at least is receding, which obviously is great news.

What's interesting, I think, also, is if you look at that blue line, that shows—that's a metric from Goldman Sachs that shows how locked down the economy is. So, the lower the line goes, the more open the economy is for business and the more free people are to travel and shop, et cetera.

And you can see that that line actually never really went up during the Delta wave. You know, and of course, it went way up early on, a year and a half ago when the pandemic really got started. And what that tells me is that we're learning to live with this pandemic without having to shut down the economy.

Obviously, we have to wear masks and people are vaccinated. But this is, to me, a very good sign that this is becoming more of an endemic than a pandemic and that, you know, that the threat to the economy at least is now kind of a passing storm.

So, you know, the flip side of that is that there won't be quite be that dividend of a reopening economy now that that delta wave is coming down. But still, I think this is a really good outcome.

And it's interesting. You know, I live in Boston, of course, and in recent weeks, I've never seen Boston so busy. It's like, where are all these people coming from? Of course, we had the marathon and now we have the Regatta coming up. But there are people everywhere. There's cars everywhere. And you know, the city is booming and I'm hearing the same thing about other cities.

It's just interesting to note, because a year and a half ago or a year ago, you know, you read the newspapers and kind of the big cities were sort of declared as, you know, their time had passed and everyone is going to move out of the cities and they're going to be ghost towns. Well, I don't think that has happened. I think it's nice to see that cities are being very vibrant again.

JIM: Yeah, for sure. I think that's part of that return to normalcy that everybody is and was really hungry for and anxious to see, so it's great to hear and to see that it's starting to happen.

And speaking of return to normalcy, I wanted to ask you one more follow-up question before we start the cybersecurity conversation. Just because we sort of started talking about risks and I mentioned inflation just a couple of minutes ago. I was hoping you could catch us up on the front, the inflation front, maybe through the lens of current labor shortages nationwide.

JURRIEN: Absolutely. So, you know, that is also the good news is that the pandemic obviously caused a severe lockdown in the economy and then we had the recovery, the reopening, as I just described. And we're basically back to now pre-pandemic levels of economic activity. So, if you measure it as the output gap of the economy, which is not what this chart shows but we've shown that in the past, that gap has pretty much now been erased.

Another way of looking at it is in the gray line in this chart, that's the gap between the unemployment rate and what is considered full employment. There's always some unemployment because people are moving around and things like that. And you can see that gap has now gone from 10.3% to 0.3%, so almost back to that pre-pandemic starting point, if you will.

And then the orange line which shows the number of unemployed per job opening is actually now all of the way back to where we were before the pandemic. And this is really fascinating because you look at those purple bars, that's the quit rate. So, that's the number of people quitting their jobs. We've done a whole show on this, the great resignation, right?

4.3 million people. And this kind of speaks to the inflation narrative, which we've also covered many times. And, you know, are we going into an inflationary period or are we in a stagflationary period which generally is defined as slowing growth but rising inflation? And what this chart tells me is that I don't see stagflation is very likely but I do see an ongoing economic expansion with some inflation as the most likely outcome.

As you think about it, 4.3 million people would not be quitting their job if they didn't have a sense of confidence that there are other jobs out there paying higher wages because otherwise, you're not going to really quit your job.

So, to me, this is a sign that the economy is very strong and that labor, of course, the labor market is a relatively sticky source of inflation. Companies aren't going to reduce wages, you know, next month just because they filled a job. So, I can see that this is going to be a part of the—of our landscape.

And of course, the Fed knows this. And the Fed is on schedule, if you will. It hasn't announced it yet but the expectations are that the Fed will soon announce the taper, right? It will start tapering its asset purchases. It's buying $120 billion a month still. But the thinking is that starting in November, which is next month, they're going to start reducing those purchases by $15 billion a month until they are done with asset purchases by the middle of next year. And then they're going to start raising rates at the end of next year. That all actually makes perfect sense because as you see, that output gap is gone, so the need for the Fed's kind of emergency policy response really—you know, it's not justified anymore. So, the Fed now needs to take that punch bowl away. And I think the markets generally are okay with that.

JIM: Excellent. As always, a fantastic recap to start us off on this Tuesday.

Leanna, I turn to you now. Sort of—everything Jurrien just managed to fit in in just six or seven minutes there is just the tip of the iceberg of what investors maybe need to or should be thinking about maybe every day or every week. Add to that the threat of cybercrime or how to protect your assets online and it can seem kind of overwhelming, I think. So, maybe if you could start us off with that part of today's discussion, sort of a high level look at what some of the risks are that at the very least, we should be aware of.

LEANNA: Absolutely. And it's such an important topic and I'm going to share some client stories in a bit. But so many have the feeling of this can't happen to me while also I know people really recognize how much of a potential threat it can be to your personal financial data and your assets. But I think it's really helpful to understand how these crimes are committed and who's committing them as well so that you can all better defend yourselves.

JIM: Yeah.

LEANNA: So, many of the thieves—we're going to call them thieves throughout this, which they are—are highly skilled and sophisticated. So, it could be individuals. It could be coordinated groups that are using technology to steal, whether it's money or your personal financial data to then log into various accounts.

So, it's helpful to know how the cybercriminals operate and there's really two camps of those.

So, first is indiscriminate targeting.

I just want to pause for a moment. I hear an echo. Am I okay on your end?

JIM: Yeah. You sound fine to me.

LEANNA: Okay, great. These are those that are casting a wide net with phishing scams with the hope that getting quantity of potential victims will yield an economic benefit. So, we hear about those a lot—I'll talk to them in a bit—and then we have the criminals targeting specific people. And we often see they're targeting high net worth individuals.

In many of these cases, the criminals are spending a great deal of time and effort identifying the target, developing a victim profile based on their information, public and private, going through their records, credit information, social network, and gathering anything for their accounts.

JIM: Lots of ways, unfortunately, for your private information to end up being visible to the public. I think social media is one great example. Be careful about what you're putting there about where your second home is, for example, or where your time share is. The more information you are putting out there means the more information other people have.

What other ways can these thieves, these criminals, these bad guys get access to our information?

LEANNA: So, we see a lot of—a common scenario. Just to walk through how it works. So, the most common we see, first, is the thief sends an email with a link or an attachment to the victim that appears to come from a known party. The targeted victim then clicks on that attachment and that includes software, malware that then infects your computer is how it would work. The thief then uses that malware to steal log in credentials of your financial accounts or any of the information you have on your computer. That then provides—the thief can then log in as the victim.

So, they would then, step three, really having access to the accounts, they can then change your profile, change your financial institution. We've seen passwords being changed. And then where we see most, the actual crime is transferring the money out with that information.

So, I've heard a bunch of different scenarios but a client recently shared that—or we saw, like, we'll see an email come in and it says something that looks from a trusted contact of, I'm in a meeting, I can't talk on the phone, but can you please wire X amount from this account to that? And the email that we get is the client's email. So, it means that they were able to log in and do things of that nature. But that's why so many firms, we wouldn't be able to act on a request like that. Things do need to be verified over the phone, two-factor authentication. We'll get into all the ways to protect. But those are different scenarios I see.

And then another one to bring up is just on elder financial abuse and care. So, we've often seen caretakers who are spending most of their time with clients as their caretaker can then gather financial information about them to then use and use the funds that way.

JURRIEN: You know, it's interesting. As my own personal anecdote, and it's one that I think many people can relate to, but during the pandemic, I got an email from the person living in a house that I lived in twenty years ago, so the current owner of that house, and actually he found me because he has a Fidelity account. And you know, Jurrien Timmer is at Fidelity and that's how he found me because I don't know the person.

But he got a letter I think from the government, from the state of Massachusetts, confirming whether he had applied for unemployment benefits, like his pandemic unemployment benefits, which of course I didn't because I'm fortunately gainfully employed.

But I know that many people had that same thing. And so, you know, there were all these protocols to deal with that and the fact that, you know, the mail was sent to my house from twenty years ago gave me some comfort that maybe this was a really old hack and not—because obviously it had very dated information. But it does show how these things can hit home.

Just one other little example. You know, I have a Twitter account, the Fidelity Twitter account where we're very active. And accounts like that—well, they don't get hacked but they get duplicated. And then the duplicate accounts will send direct messages out to the followers of that account. And you know, we have—I have 70,000 followers. And they're usually scams usually involving crypto, unfortunately. That's another area where you just have to be super diligent about these things.

JIM: Yeah, a similar thing happened to both my wife and me during the pandemic. Someone applied for unemployment benefits in both of our names. It was just a real mess. I think it was six months apart it happened. We're still continuing to clean up the mess from that. Unfortunately, we all have unfortunate examples to share.

I switched my mic so hopefully the echo went away and it sounds better. I hope it does. Great. Okay.

So, Leanna, we talked about the bad stuff. Now can you give us some suggestions and tips on what to do to protect ourselves a bit more?

LEANNA: Yes. So, a lot of these are a given. But I really can't tell you enough of how many clients will tell me that they do have the same passwords for their shopping account as their financial account, for their streaming account as their financial account. So, I'm going to share a story in a moment.

But first is make passwords long, strong, and unique. For those that say, I have no way to remember all those log ins and passwords, there are password managers out there. But passwords truly are the first line of defense. Never use names, birth dates, Social Security numbers, personally identifiable information. You know, I was chuckling before this. Like, family members that just use their kids and birth dates. Obviously, those can be a given.

But recently a client shared that he had had his streaming account the same password of his financials. And his daughter went off to college and his daughter was sharing the password of their streaming account, you know, watching shows during school, and that password just got passed along. And then at Fidelity, we got an alert of a different computer trying to log in to different accounts. So, it just shows, it's completely innocent in nature, but someone has the password in the wrong hands and that's where we can see the crimes happen.

Another big thing, just make passwords long and strong, ten or more characters using complex combo in characters. And like I said, again, the password manager is really important.

And then at Fidelity we have this, but two-factor authentication adds that layer of security. The other financial firms have this as well. It's just an additional way to keep your account safe.

And then this one was actually a learning for me, is just keeping your computer systems up to date. So, software makers, they have teams of cybersecurity specialists and they can go in and install updates and patches. It's just a way to, again, further secure your accounts.

JIM: That's great. I can't say enough about two-factor authentication. I didn't even know about it until a couple of years ago. I learned about it here at Fidelity. It's a really quick setup. And if I ever try to log into my account from another computer, not my regular computer, I get a code on my phone that I have to put into that computer.

That means if somebody else tries to access my account from their computer, two things will happen. They can't get in because they won't get the code, but I get the code so I know that someone maybe has my password. So, you feel pretty protected doing that.

LEANNA: Exactly that. And it's always scary when you get those texts because you're thinking, well, I didn't log in. But again, it makes you feel safe having those. And there's also the My Voice. A lot of people have—a lot of firms have the voice verification. That's just another way to keep your account secure.

JIM: Jurrien, just in the couple minutes we have left, what's your sense of sort of the larger impact of cybercrime? I'm thinking for example, a company gets hacked, it's a big piece of information that's got to affect stock prices, for example. Does that ever move the whole market?

JURRIEN: I don't think it really moves the whole market. Obviously, there have been incidents of, you know, companies getting hacked or their customer lists getting hacked, right. So, but it's one of those things where there's not a lot we can do to control that. Like, as Leanna said, there are things we can do to control, you know, protect our information. And companies will do the same thing to protect their information. But beyond that, other than deciding not to be invested, there really is not a lot that we can do. And, you know, we've talked about this many, many times. There are always things to worry about. And obviously, companies like Fidelity, but every other company, will be very active in trying to mitigate any risk of being hacked. It doesn't mean it can't happen.

But I have—you know, I have never seen it really impact the market as a whole. I mean, maybe if the economy gets hacked somehow, that will be a different story and maybe that would look kind of like a natural disaster. And then, you know, it gets fixed and then everything goes back online.

So, I wouldn't expect that if there isn't an event that would happen, like a cyberattack by another government or whoever, that it would last more than kind of a limited period of time.

And then I go back to the long-term. We're all long-term investors here and you know, this chart, which shows that I spend too much time on my hands making charts, but it shows the progression of the stock market by year over the last 120 years.

You just see that relentless march from the top—from the bottom to the top. Sometimes it goes fast. Sometimes it goes slow. And I think it's just useful when we have these conversations and many others, that we're in this for the long run and I think over the long run, it's the fundamentals that drive stock prices. And there will be things that will disrupt or interrupt those fundamentals but as long as they don't change them, I think, you know, we'll be fine.

JIM: Great. Fantastic advice and context from both of you, as always. So, thanks for making time, again, to be with us this week.

For folks watching, thank you again for making time as well to be with us. Just a reminder that if you need help with your financial planning or you have questions about how Fidelity can help, you can certainly download our app or visit our website. You can do keyword searches there to learn more about cybersecurity, cyber safety, for example, or any other financial topic that you might be interested in. It's a great way to continue learning about what Fidelity has to offer.

A huge thanks to Jurrien and Leanna and we hope to see you back here next week.