April 7,2021

Robert Albertson | Chief Strategist, MD
212-466-7946
robert.albertson@psc.com

Company: Ordr
Bank FinTech Showcase Interview Series

CEO/Founder: Greg Murphy
Current User: Woodforest National Bank CISO;
SVP Information Security, Marc Crudgington

Category: Cybersecurity

Preview: Cybersecurity is perhaps the biggest challenge facing financial institutions. It has become a mission critical problem with an accompanying set of regulatory compliance issues. There is an ever-growing multitude of technology providers addressing these tasks. Ordr is among a handful of security and infrastructure offerings that delivers visibility and security for connected devices—identifying the risks they bring and securing vulnerable ones from cyber attacker access. So-called "agentless" devices posing this risk are extraordinarily numerous and too often overlooked. Phones, Wi-Fi printers, laptops, and security cameras are just a few examples of these access entry points to a financials systems network and data. These "Internet of Things" (iOT) are increasingly being compromised by bad actors. Eliminating these risks requires a massive, complete inventory and monitoring of all such devices. Unique to Ordr is the ability to learn the unique communications patterns of every device, then proactively create segmentation policies to ensure devices have the access they need while limiting exposure.

Robert Albertson: Joining us is Greg Murphy, the founder and CEO of Ordr. Also joining this interview is Marc Crudgington, CISO, SVP Information Security of Woodforest National Bank an $8.6B asset bank across 17 states with 768 branches.

Greg, we will start with you and thank you for this opportunity. Let's begin with your background and how you came to lead Ordr? Where did you begin your career?

Greg Murphy: I began my career 20 years ago, I started a company that was focused in wireless network management, and helping large organizations manage their Wi Fi networks. And through that, I came to understand what it took to build a software focused organization, but also gain an appreciation of just how challenging networking and security are for enterprises. I was very fortunate to build that company and then sold it in the early 2000s to Aruba Networks where I then stayed in a number in different roles for the next seven years until we in turn sold Aruba Networks to Hewlett Packard. And at that point, having had that experience, I was looking for the next great challenge in my career and that turned out to be helping organizations solve the network or connected devices security.

RA: What year did you begin?

GM: Ordr began in 2016. We've been in business for four and a half years now.

RA: Could you briefly describe your organization?

GM: Sure, we are a Silicon Valley based company headquartered in Santa Clara, California with just under 100 employees. While Ordr is based in California, our employees are scattered across the United States, Asia and in Europe.

The company is really one that was **founded by industry veterans who have built some of the largest networking and security companies in Silicon Valley like Cisco Palo Alto Networks and Aruba Networks.** The Ordr team has had a lot of success in their previous careers, and know how to grow large companies. Our leadership team understands that the way you grow is by focusing on the needs of the enterprise customers.

RA: I am fascinated by the fact that you began quite successfully building Ordr with users in the medical community and currently count the Cleveland Clinic, and the Mayo Clinic as clients. Why was this one of the first sectors for you, and why are you now expanding into financial services?

GM: Sure, it's a great question. When we started, we understood that one of the biggest challenges facing any enterprise today is that there are a huge numbers of devices connected to their networks. These organizations **don't know about these devices nor are they able to identify or understand the behavior of these devices.** That problem applies across almost every industry. What we experienced in healthcare, was that many of these connected devices were really mission-critical medical devices like MRIs, infusion pumps and patient monitors. These devices were crucial to patient care and outcomes.

You can imagine if you're the CSO of a hospital system, you need to know exactly what's connected to your network. If something impacts the operation of an infusion pump that is pumping drugs into a patient that is a very, very serious issue for you and for your organization. As result of this possibility almost every CSO or security officer in the medical community became very concerned about medical device security.

A few years ago the WannaCry virus (a massive security breach globally in 2017) was really a galvanizing event that was spreading like wildfire through a number of hospitals. This virus took entire systems for ransom and forced many of those hospitals to revert to pen and paper for a number of days or even weeks because so many of their critical medical systems were impacted by WannaCry. That woke up the medical industry that this was not just a theoretical problem, but a very real-world problem that could affect the continuity of their operations and their ability to do business. **The medical world, you know, awoke to that reality quite early, but if you think about financial services it shares many of those same characteristics, with the healthcare industry.** There are just a huge number of networked devices in a financial services institution, or retail bank. At a typical institution there are connected devices everywhere: door locks, the security cameras, the ATMs, networked desk phones, your monitor's surveillance system. There are lots of connected devices, frankly, a lot of those are in very highly distributed environments where there are not the local IT staff or security staff in place.

Financial services is, obviously, a very heavily regulated environment where there are very strict compliance concerns. Healthcare is almost identical in that respect. **The cost of a breach in both a financial services institution or a healthcare facility/institution can be astronomically high**. The combination of very distributed organizations, large numbers of mission critical devices, a regulated environment and the costs of breaches makes device security an absolutely critical issue in both the healthcare and financial industries. **What all these organizations need is very similar - to understand exactly what's connected to their network**. They need to understand where those devices are, they need to know how they're behaving. They need to be able to identify if a device is behaving badly, very quickly. Finally they need to be able to lock down those devices to ensure that they are protected and that no malware gets into the environment. Malware can spread like wildfire and take down the entire bank or the entire hospital. While the two industries seem very dissimilar on the surface, their security requirements are actually quite similar in many ways.

RA: You make a strong point. Having been in the banking industry all my career I'm glad you're now part of the solution.

GM: We're going to be.

RA: How are you funded and what are your needs as you expand among other sectors?

GM: We're very fortunate that we're backed by some of the leading venture capitalists in Silicon Valley and around the country. We are funded by Wing Ventures, also by 1011 Ventures. Our most recent financing round was led by Battery Ventures, and then joined by the Mayo Clinic, and by Kaiser Permanente Ventures. That last financing round brought our total funding to date to about $50 million dollars in the early part of 2020. We're very fortunate that we have the capital that we need to expand and grow the organization on a global basis. Where we're continuing to invest is obviously in R&D to move the product forward, but also in marketing to spread the word about the solution and educate customers about what's possible. We look forward to expanding our partnership with PSA and obviously to reach new markets worldwide.

RA: Let's begin with your definition and explanation of "agentless devices", included are IoT (internet of things) and give some examples of those. Perhaps explain why they are so often overlooked or difficult to follow. What is the key challenge? Take us into the weeds a bit here please.

GM: Sure, if you look at the world from the lens of a traditional IT perspective; devices were relatively straightforward for a long time . There were PCs and workstations and tablets and mobile devices, where there's usually a user associated with that device. If IT or network security professionals wanted to get visibility and control over that device it would be pretty easy to do. I would put a software agent on a laptop or a mobile phone and would be able to understand what that device is doing and would have control of that device.

The problem is that when you look at today's network, **the number of connected devices is growing astronomically.** These devices consist of what I consider the "other" category of non-traditional devices like building management systems, medical devices in healthcare, manufacturing devices in the industrial sectors The number of those devices is actually dramatically outgrowing the number of traditional IT endpoints. The problem with these devices is that there are so many of them from so many different manufacturers with very proprietary operating systems. It becomes extremely difficult to manage visibility to those devices with a software agent. It's just an impossible task when you look at how many millions of devices could be connected in a global 2000 organization. Traditional tools that IT organizations use aren't very effective in protecting these devices, and the only real common denominator is to leverage and use the network and the existing infrastructure, like firewalls, to regulate and control what these types of devices can talk to and how they can communicate on the network. So if I can't put software on the device, I'm going to use my network infrastructure to protect those devices.

The network will then, in turn, regulate what they can do. Traditional solutions, just a software-based or an agent-based solution won't work, and traditional networking tools don't have the depth of understanding of what these devices are and how they behave. How can I be protected effectively if I can't tell the difference between a Philips Lighting System, and a Philips MRI? It's awfully hard to define your policies as to what each of those devices should be allowed to do on a network.

RA: To better illustrate the risks from these devices would you give us a couple of actual examples, you came across when deploying your platform? What were the findings or challenges that the Ordr systems control engine addressed?

GM: Absolutely. When I talk to CSOs I always ask them one question which is “How confident are you that you know what's connected to network?” I've never had a CSO say that they were 100% confident that they knew exactly what was connected to their network. The reason for that is that a lot of these agentless unmanaged devices that we're talking about are very often purchased and connected by organizations outside IT. For instance, facilities may install a new elevator that IT does not even know is connected to the network. We went out and did an asset inventory for one of our clients. We found a security gate in their parking lot. They had absolutely no idea the gate was connected to the network and unfortunately that security gate was infected with malware. This malware was in the process of infecting their entire organization. IT would never say to themselves, “Oh that security gate in front of our parking lot, that's a network connected device” but in fact it was.

You have users that bring devices into the environment without IT knowing about them. In another one of our clients, we found an executive’s’ Tesla automobile connecting directly to the enterprise network getting a software update Again, another device that it had no knowledge about nor control over. Similarly, in the banking environment you may find your iPads constantly connected to the network. Some iPads may be from guests that are visiting the bank, but others might be employee tablets, others might even be used for signage. They are all iPads, but have very different behavior patterns. You need to be able to understand those behavior patterns to apply the rules and policies appropriately so that the guest’s iPad is given different permissions than an employee’s iPad. It really comes down to understanding exactly what these devices are and how they behave. This allows you to make intelligent decisions about how they can be protected.

RA: Marc, I think this is a good time to bring you into the discussion. Can you tell us what security challenges you were looking to address at Woodforest Bank? Give us a little bit of your perspective.

Marc Crudgington: You do not realize how expansive your network is until you inventory every connected device. My objective when entering the banking world 8.5 years ago was to make security more intelligent and efficient. A device as simple as a badge reader can be used to compromise an enterprise network. So the main thing we were trying to address is the security around a lot of these agentless devices that Greg mentioned. We started to search for a traditional IoT platform that could help improve our security posture.

But the interesting thing as we dug into it a little bit more, and specifically looked at Ordr is that **it is not just for IoTs. It's anything that is connected to your network**, and that's what I think makes them special among peers. We talked about something we wanted that would integrate with our entire security stack. This intelligent system is what I kept going back to - we need efficiency and security.

Here we searched for three things: For people, for time and dealing with too many alerts. That makes what I call the “mitigating the breach to breach response” gap very difficult. The time between when the threat actor enters your environment and the time you're able to detect it and start remediating. Smart systems, like Ordr, can help. They help you reduce that time which is very critical because threat actors can pivot around your network very quickly. Especially the sophisticated attack groups that are going after financial services. We've seen many of those breaches over the past few years. Regulators don’t tell you what system to use. They just say you have to protect your customer data, and you have to know all the assets that are on your network. Ordr can help in any of those areas.

RA: Marc, I'm curious when Ordr did come into your bank. Did they show up with many surprises in terms of vulnerabilities, once they got underneath the hood?

MC: I can't get too much into the weeds around that Robert. I was not on the management team then. I will tell you the surprises. We had a lot of devices that we had connected that we were not managing effectively. Like I mentioned, you badge-in every day. You have a badge reader, you have a kiosk you have to walk through. Ordr made us realize that all these devices could provide access to the network.

Using network architecture to help protect devices only goes so far if you don't do the things like profile device behavior and understand if your entity has vulnerability. **The Ordr platform gives you that visibility to understand how that device is being used**. We anticipate that a lot of agentless devices have vulnerabilities. Some of them show up with our vulnerability management tools and some do not. The Ordr system allows us to see vulnerabilities in agentless devices unlike traditional solutions.

We felt that Ordr would improve our security posture, and just assist us overall. Ordr integrates very well with our security stack, specifically Cisco ISE, and **the outcome was just a fantastic win for us.**

RA: Impressive. Marc, once the device anomaly presents itself, what kind of automatic responses occur?

MC: Ordr has automated responses to threat types that we can create internally with our security team. The Ordr team helped us in that customer success endeavor. There are a number of things you can do based on the enforcement of the policies that you input. Visibility into the effected system and what you should do is step one, and Ordr certainly helped quite a lot with creating automated responses to certain device behaviors. An Ordr equipped CSO or IT team can go as far as they need down to disconnecting that device based on your policies and procedures.

If I did have a device that, let's say, is going rogue, I could disconnect that from our network. Depending on the other policies and systems you're using, I could segment that device. So I think their platform gives you the visibility along with the policies that you can put in place to thwart any type of activity. Getting back to what I talked about earlier, saving that efficiency and your team, then you can follow up and determine what were some of the causes.

GM: Just to add to that, when anomalies present themselves, there are two modes you can think of. One is a reactive response as Marc was talking about - If you see a video surveillance camera talking to one of your other business systems or to a server in Russia, we could immediately shut off that communications flow since that's not a permitted behavior. You can do that without taking the device offline. The second mode is a more proactive security posture. You can deploy software to the camera that says these are the only things it's allowed to do. These are the only destinations that that camera should be allowed to talk to inside your network, these are the only protocols that it should be allowed to speak and be able to apply those policies so that it **becomes impossible for that device to break out of its permitted behavior**. That type of segmentation can be very powerful in ensuring that the most critical business systems are protected.

MC: That is on the preventative side and that is another facet to the Ordr system. If we can prevent something from happening it saves our team time. The security team no longer has to triage and look after the fact, even though it may have been segmented or it may have been disconnected from the network or whatever that response is. Ordr keeps us from having to respond based on those policies. That is the granularity that Ordr gives us.

RA: Greg, this sounds complicated. More so than I think most people realize. Could you walk us through a typical installation? How complicated is it really and what are the typical issues? How long does it take? Are there any conflicts with legacy systems? What are the challenges?

GM: It sounds complicated because understanding all of the devices that can be connected to an enterprise network at scale and understanding all of their communications is not possible without the help of software. It really is beyond the capabilities of a human team. Marc spoke about badge readers as a point of entry. I mentioned security cameras and HVAC systems as other agentless devices. There's no human being who can carry around all that in their head. With Ordr, you have knowledge of how all of those devices should behave, and then can use that information to generate policies.

The way that we **simplify and eliminate that complexity is by using AI, and by using machine learning** to understand all and identify all of these devices and understand their behavior patterns.

When we go into an environment, the solution itself will be installed and set up within hours. At that point Ordr is passively monitoring the traffic on the network. This avoids the needs to install software on all of the endpoint devices. Ordr SCE watches the communications flows as they move across the network and we use the deep packet inspection of that traffic to identify and classify the devices.

Within just a couple of days we've got a very deep classification and understanding of exactly what devices are connected in that environment. Ordr then builds up profiles on how those devices behave. These Ordr-created device profiles help CSOs understand the difference between for instance, how an HVAC system behaves and communicates on the network versus one of your media systems. Ordr installation starts with very fast identification and classification of the devices, and then over a period of days builds the behavioral models of those devices.

After this initial stage is completed we can identify any potentially anomalous behaviors that occur in your system. Ordr is designed to complement existing systems and existing infrastructure; no bank, no financial institution is going to have the luxury of going and replacing their entire switching infrastructure their entire wireless infrastructure and all of their firewalls. A complete overhaul like that could be 10s of millions of dollars.

Ordr is designed not just to integrate with the system, but to leverage them and to use the capabilities that they've got to be able to protect all these connected devices. Ordr SCE sits on top of an existing infrastructure and legacy systems, and uses the capabilities that are already there. This is a much easier implementation rather than forcing a complex network or security upgrade on an organization.

.

RA: How do you structure pricing with your clients?

GM: The Ordr solution is a SaaS solution. The price of the subscription is based on the number of employees or the number of devices that we find in a given enterprise environment. So it's a pretty straightforward SaaS licensing model.

RA: This goes to both Greg and Marc. If I'm a bank CEO or CSO what are the necessary components that I should be considering for a complete cybersecurity defense system? What should I have in place that will comply with the current regulatory requirements? Where do most financial institutions in your mind, fall short, with respect to the regs?

GM: I'll take this one, Marc. No matter what cybersecurity framework your organization has adopted, no matter what regulatory framework is in place - regulators almost always start with an assumption that you must have an accurate inventory of what you have on your network. The very first thing that a regulator or auditor is going to ask to see is this device inventory. As I said before, if you don't know about that device, you don't have visibility into that device and there is no way that you can possibly be securing that device. If you can't see it your security framework immediately falls apart.

I think the starting point for any, any cyber security defense model framework has to be for good, accurate inventory of what's on the network. The other core component that I would point to in almost every security framework is that it requires some form of segmentation, which is to say that you want to be able to control where devices are on your network and what other destinations they are allowed to communicate with. In order to segment you need to make sure you understand what the devices are so I can say okay, a guest iPad that should only be allowed to be connected to my guest network and should never be allowed on to my enterprise network.

Financial institutions are usually pretty good about segmenting. **Banking firms are good at separating banking related networks from the enterprise network, but very often they're not as good with securing the enterprise network.** These banks need a system to make sure that the facility's equipment is separated from the physical security equipment, and other classes of data. It's really all about starting with an accurate understanding of what you have, and then using that information to define where these devices should be allowed to sit on the network and what communications privileges they should have. Marc, Is there anything that you want to add?

MC: Yes, I would definitely agree with that and from a CEO perspective or the board even. The asset discovery is extremely important but understanding what risks are around those assets is critical. Not all assets should be treated the same. If you don't have an individual profile for each asset your system treats them the same. You know that our core payment system is not going to be treated the same as another system that doesn't contain the same type of data, or the value data from a regulatory perspective and how CSOs should approach things.

It's always continuous, continuous improvement. Continuously evolving your institution's program. Ordr is a tool that can help your institution evaluate your risk, setting up your strategy. The world of IT is constantly changing. We are in an era of advanced threats in a dynamic environment.

I would also say that, risks associated with 3rd of 4th party vendors are also crucial to understand and quantify. What ports do these 3rd or 4th parties want you to open. What are the connections and the API's that connect the entities, and what risks are associated with those connections? **Regulators are starting to get smart to 3rd or 4th parties opening the regulated institution to risk**. You have to stay ahead of them. Do you know where each of those devices are? Are you continuously improving your process? Ordr helps us stay ahead of not only regulators, but also threat actors.

What you hear about now is zero trust. Zero trust covers your enterprise networks that you're trying to protect. If you adopt a zero trust framework, specifically around assets in this case, **you would be ahead of 99.9% of the other companies that are out there.**

RA: Greg, does any legacy security exist, anything which tracks devices in a similar manner as yours? Do you have other credible competitors in your space? I see some of the differentiation but it almost sounds like you guys are the only ones doing it.

GM: There are definitely other organizations that try to provide visibility into what's connected in a network environment and to protect those networks. I point to legacy solutions like Network Access Control System. Very often those solutions don't have the depth of understanding of devices that Ordr does. To them from a network perspective when they see a device it's as an IP address or a MAC address. This data identifies the device, but that doesn't really tell you what's the make, model, the software version on the device, and that's really what you need to know in order to understand what that device is, how it should be behaving and what vulnerabilities the device might have. **That is where I think we differentiate ourselves - is not just an identification system. Ordr sees there is a device connected to the network, identifies that device, and then by marrying that with an understanding of the device behavior, and allows us to help automate and generate those policies**. That's what I think really distinguishes our solution from others that the depth of visibility, the understanding of the behaviors of these devices, and the ability to use that knowledge to translate it to policies that can be used to protect those devices.

RA: Marc, can you share some of the reasons that you chose Ordr over the alternatives?

MC: Yes, definitely. Greg hit on some of those so I won't rehash them, but I looked at it from a couple of perspectives. One was our existing technology stack and how Ordr would fit in our existing system. I mentioned one of those Cisco ISEs. That played a big part in our decision.

I also looked at Ordr as a company, and I looked at some of the people that would be helping us out along the way. I also looked at their investors and their board, and their backgrounds. Greg mentioned Wing (Venture Capital) and Peter (Wagner). I've kind of followed him a little bit from my past in the Silicon Valley. One of the companies that he helped fund was Redback Networks, which I was very interested in at the time. I understood that these guys would not invest in a company, unless they truly believed in it and it had viability. I knew that this was a long-term play. It was a company established with vision or direction, and had great support from professionals across Silicon Valley. That gave me a lot of comfort in investing or becoming a partner of a startup company.

Ordr believes in customer success and has an executive devoted to customer success, which is very important. Three of my top vendors have great customer success teams and I would go to bat for each of those vendors anytime I'm asked to. Ordr fit in that same mode of believing in customer success, which is essential when you get the product and decide how you are going to utilize it. Is it going to become shelf ware, or are you going to be one of those companies that uses the system to its full potential.

RA: Bank regulators require a lot of documentation for things like this. How do you help organizations to produce that documentation, and to what extent have you been interfacing with bank regulators all along?

GM: **We have definitely been working with regulators, auditors, and consultants in order to understand just what they are looking for.** What information do they need when they go into a financial institution? That's how we really built the product and one of the areas where you see that is in our reporting capabilities. That includes the ability to quickly and easily generate a report of inventory, for example of what's connected to my network and what software version is running. We have dashboards that regulators will take a look at that show you all of these devices and assign a risk score to them. This allows the organization to explain exactly what devices have the greatest risk and how they've been using that information to prioritize their security programs.

Ordr gives institutions the ability to demonstrate these programs that you've put in place are working. Because we monitor the traffic and monitor these networks on a day in day out basis we can show that devices that are on the facilities network are not able to communicate and have not been able to communicate with devices on the physical security network. **We can show and prove that the policies that have been put in place are actually having the effect and the impact that they're supposed to.** Fundamentally what regulators and auditors are looking for is that you have processes in place to understand risks, and you can show them that the programs that you're putting in place are doing a good job of reducing risk and protecting the organization.

RA: Marc, would you share the Woodforest experience with Ordr? Please highlight some points I may have missed in the session.

MC: It's been a great experience. We started the journey maybe six to nine months ago or so, and so far it has been a great experience. Obviously I wouldn't be here if I didn't believe in Ordr and didn't believe in the product and what they're trying to accomplish. I will say from the get go they have all done a fantastic job. From the on-boarding process, getting the information we needed from them, to the regulatory side where Ordr provides us with reporting that goes to regulators.

Ordr has worked with financial companies before us, but they were very complementary and providing us the things that we need. The ask can be onerous at times, I will admit that, but It did not take us very long to see the value. During the proof of concept, proof of value that we went through that we were dealing with a very sophisticated system and that it was just the type of system that we were looking for. We just felt that it was a great fit for us.

In terms of surprises along the way; there haven't been any hiccups. You typically run into a lot of hiccups when you're implementing certain solutions, but it's been a successful journey so far and we look forward to continued success.

RA: Marc, we really appreciate you being here with us. It's unusual to have a user melded into a discussion like this. I find it very helpful myself. Greg last question. What pushback, if any, have you received when you're pitching to bank clients?

GM: I think that the only pushback that we hear sometimes when we talk to banking clients and they hear organizations talk about us as an IoT security provider. Sometimes banking institutions don't consider themselves to have big IoT initiatives, they think about IoT as something for the manufacturing sector or industrial or for healthcare. But when we sit down and we talk to the financial institution, and start to talk about all of the different types of devices that are connected in their environment, they understand they do have hundreds of thousands of these unmanaged devices: the cameras, the televisions, digital signage, the IP phones, kiosks and your badge readers as Marc was talking about. I think sometimes the financial services institutions don't think of themselves as having a major it IoT initiative.

The other area where we sometimes hear a little bit of pushback is when clients say “The problem seems so big, where do we get started with hundreds thousands of devices. How do I start to bring those under control.” That's really where we can step in and provide value. We explain exactly where these devices are and what they are. We then help organizations prioritize and understand which of those devices are truly the ones that are business critical. Them we determine which of them have vulnerabilities that really need to be addressed quickly. It's really helping organizations understand that the task is not insurmountable. It's just a question of understanding what you have and figuring out where to get started.

RA: Let's conclude here. I think it's been a very thorough and impressive discussion. Greg, if a financial institution reading this session would like more information or to connect with you, would you be okay providing your phone and email coordinates here? I want to thank you both very much for your time. It was a pleasure.

GM: Absolutely, thank you and thank you for the time. Absolutely. Organizations can contact me directly.

My email is GMurphy@ordr.net.

General Information and Disclaimers

This report has been prepared and issued by Piper Sandler & Co., a registered broker-dealer and a member of the Financial Industry Regulatory Authority, Inc. The information contained in this report (except information regarding Piper Sandler & Co. and its affiliates) was obtained from various sources that we believe to be reliable, but we do not guarantee its accuracy or completeness. Additional information is available upon request. The information and opinions contained in this report speak only as of the date of this report and are subject to change without notice. Contact information for Piper Sandler & Co. and the author of this report is available at www.PiperSandler.com

This report has been prepared and circulated for general information only and presents the author’s views of general market and economic conditions and specific industries and/or sectors. This report is not intended to and does not provide a recommendation with respect to any security. This report does not take into account the financial position or particular needs or investment objectives of any individual or entity. The investment strategies, if any, discussed in this report may not be suitable for all investors. Investors must make their own determinations of the appropriateness of an investment strategy and an investment in any particular securities based upon the legal, tax and accounting considerations applicable to such investors and their own investment objective. Investors are cautioned that statements regarding future prospects may not be realized and that past performance is not necessarily indicative of future performance.

This report does not constitute an offer, or a solicitation of an offer, to buy or sell any securities or other financial instruments, including any securities mentioned in this report. Nothing in this report constitutes or should be construed to be accounting, tax, investment or legal advice.

Neither this report, nor any portion thereof, may be reproduced or redistributed by any person for any purpose without the written consent of Piper Sandler & Co.