Filed by L&F Acquisition Corp. pursuant to
Rule 425 under the Securities Act of 1933, as amended,
and deemed filed pursuant to Rule 14a-12 under
the Securities Exchange Act of 1934, as amended.
Subject Company: L&F Acquisition Corp.
Commission File No. 001-39722

The following is a transcript of a webcast interview first made available on April 26, 2022.

John Jannarone: Good afternoon. Thank you for joining. I'm John Jannarone, Editor-in-Chief of IPO Edge, here with a fireside chat, a special event. We have three guests today, two of them the founder and CEO along with the CFO of ZeroFOX, and the CEO of L&F Acquisition Corp., which, of course, is taking the company public through a SPAC transaction. It trades on the New York Stock Exchange under ticker LNFA. You're going to meet all three of these gentlemen momentarily. You're going to hear about how cybersecurity is changing, a recent acquisition the company did, which is transformational that's really going to open a runway for growth, and future other growth opportunities through M&A and through organic means.

Before we bring the guests on, I'd quickly like to take care of a little bit of housekeeping. We strongly encourage you to ask questions, and we'll save some time at the end for that. The easiest way is to pop those right into your Zoom portal. All three of us, or I'm sorry, all five of us, we'll see those and we'll get to them later on. You can also shoot an email to editor@ipo-edge.com. We can pick it up there. And lastly, if you'd like to watch a replay, it'll be up an hour or so after the event is over on ipo-edge.com. You can also look up LNFA on Yahoo Finance or your Bloomberg terminal, and you'll find it there as well.

Now, one last thing before we bring on the guests. We're going to give you an overview, the business with a really good video here they've shared with us, and we're going to let that play now.

Video: Security teams are expected to be defenders, innovators, and firefighters, all in a 40-hour work week. Meet ZeroFOX. Stop digital firefighting and start disrupting adversaries before they strike. ZeroFOX gives security teams proactive protection to act quickly, disrupt attacks and predict what tomorrow will look like. Don't just identify threats. Stop attackers no matter where they lurk. With the power of AI, gain total threat visibility and the tools to take action. ZeroFOX protects your public attack surface by dismantling attacker infrastructure. No more waiting on attackers to make the first move.

Find leaked credentials on the dark web, take down impersonating phishing sites and neutralize external threats to your brand, all in one comprehensive platform. With more than a million disruptive actions in three months and a time to response measured in seconds, ZeroFOX churns through massive data loads to identify the specific threats targeting your business and executes take-down orders for you. Receive the confidence your information, brand, executives and domains are safe and secure. And with the ever-changing digital landscape, rest assured you're always one step ahead of the bad guys.

Hundreds of threat experts fight by your side, monitoring the dark web for early signs of attack planning and emerging cyber tactics, giving you finished and actionable intelligence to make smarter decisions. That's protection and intelligence to fight off today's digital attacks and prepare for what's coming tomorrow. Don't just respond to threats. Go to war and win with ZeroFOX. Protection to secure today. Intelligence to predict tomorrow.

John Jannarone: All right, that was great. Now I'm going to pass the baton to my co-editor, Jarrett Banks, who is going to introduce today's guest. Jarrett, go ahead.

Jarrett Banks: Thanks John, and welcome to our guests. We like to start things here at IPO Edge by talking to the SPAC, if we could. So we have Adam Gerchen, the CEO of L&F Acquisition Corp. Adam, let's start with you, please tell us about L&F, what it was looking for and why you ultimately selected ZeroFOX.

Adam Gerchen: Yeah, absolutely. First, let me just thank you and the team for having us on. We're thrilled to be here to talk about the ZeroFOX story. For just some quick background and context, we formed L&F a few years ago as a partnership among myself, Jeff Hammes, the former managing partner of Kirkland & Ellis, which is the world's largest law firm, and Victory Park Capital, an institutional investment manager that's really been a pioneer investing around tech-enabled industries and asset classes. Given our collective backgrounds, we expressed a pretty narrow mandate for L&F, which was to focus on the convergence of tech, software and services across governance, risk compliance and legal functions.

And when we originally IPO-ed, we really articulated three thematic trends behind our thesis. The first was the shift from analog to digital. Second, the proliferation of data, and maybe most relevant here, the increasing number of mediums or surfaces where that data resides. And third, just an increasingly burdensome regulatory environment and compliance regimes really around the world.

And so I don't think you could have an asset more on point than ZeroFOX, both from a sector perspective and with those macro tailwinds behind it, especially given this combination with IDX, which is creating the undisputed leader in external cybersecurity, really across the entire breach life cycle. So we couldn't be more excited about the platform that Foster and Tim and team have built at ZeroFOX, and we're excited for all to come as partners as we transition from private to the public markets.

Jarrett Banks: Great. Okay. And then let's flip the question for Foster and Tim. You guys have a proven business that could have considered a regular way IPO, and yet you chose a SPAC. Why did you choose L&F?

James Foster: Well, I think we had a goal, first and foremost, to make a very strategic acquisition, and that was to acquire IDX. They have been a partner and a customer of ZeroFOX's for several years now. We've known the management team, the technology, the platform, and in a large part, their customer base for also several years. And as a catalyst to completing that acquisition, we found that partnering, if we found the right SPAC partner, would be a really interesting way for us to get to market and allow us to accomplish two milestones in our company trajectory. One, get the capital fund in the next major acquisition, IDX. And then two, set us up for the long haul. Leverage the power of the public markets, leverage the power of new public shareholders and the experience they could bring to the table, and create an additional growth driver for us.

And lucky for us, when we went out to the SPAC market last year, we were fortunate enough to talk to several experienced operators that could add real value, but L&F stood out for us. They were hands down the right partner for us at the right time. We were very fortunate to meet Adam and the team that he created to back that organization, and they've been true to the pitch. They have added value leading up and through our BCA and combination, and then post, as we kicked off this year and certainly getting through our government review period here and our S-4 process. So we're excited about where we are, but that's only surpassed by the excitement to get this transaction behind us and continue to execute.

Jarrett Banks: Great. Tim, did you want to add to that?

Tim Bender: I think Foster hit it right on, that we're really excited to get into the capital markets and really expand our vision as a leader in external cybersecurity.

Jarrett Banks: Now Foster mentioned the IDX deal, which of course, we want to get into quite a bit later in the broadcast. First, let's start at the top. Foster, can you tell us what external cybersecurity is as opposed to internal cybersecurity and why is it important now?

James Foster: Jarrett, it's what keeps everybody up at night in my world right now. The years and the decade of being worried about insider theft and insider security challenges are behind us. Everybody now is worried about an external attack, somebody that does not work for you that may be sitting halfway around the world as a part of a nation state group or maybe decentralized cybercriminal group attacking your organization, for one reason or another, that may be beyond the traditional reach of law enforcement or what I just call a common law. And so we help organizations protect themselves against those external attacks.

And so the way to think about this succinctly is there is a great group of individual companies that are out there helping protect inside and internal security. Think of those as the CrowdStrike and SentinelOne. Before CrowdStrike and SentinelOne became the darlings of that internal security, also known as antivirus, next generation antivirus endpoint security, it was McAfee and Symantec, and they protect all of the organization's devices. Those devices you can hold, you can understand, you could put asset tags on. And that's what they're really good at, putting agents on devices that are owned and really securing the inside of an organization.

There's another class of security products and platforms out there called edge security. These are the traditional firewall guys, Palo Alto Networks and Check Point and Fortinet, now with the disruptive player out there and Zscaler that's doing it in the cloud, they help separate the inside of your organization and the outside. And they try to keep the bad out. The challenge is, especially with COVID, organizations are increasingly invested in digital mediums to reach their customers, to engage with their employees and partners. That happens off your device and outside of your network. Everybody went working from home, and you've got external assets now that are being attacked from outside your firewall, and your traditional agents and boxes don't work as well anymore.

And that's where ZeroFOX comes in. We help an organization understand the assets they have beyond their firewall. We help them manage them and protect them against those external attacks. And the headline is ransomware. Ransomware is the perfect example of an external attack with an external motivation to target an organization. And we're helping customers in over 50 countries today. I'm proud of the work we do.

Jarrett Banks: That's a great point about COVID and work from home and the new vulnerabilities that exist there. Can you give us, Foster, a few examples of how ZeroFOX works with its clients?

James Foster: Sure. Well, on a business model, we're an enterprise SaaS company. We've got great visibility and predictability, given our business model, into future revenues, future revenue streams, given our SaaS model. We're boring from the standpoint that we charge like Salesforce and everybody else. It's a 12-month contract, charged monthly, but paid upfront in advance in typically 12-month chunks. And about 80% of our revenue comes in one-year deals, and so about 20% is in multi-year deals.

We work with our customers at varying sizes and scope. We don't just work with the biggest companies in the world. We're not a small, a medium-sized business provider only. We've got customers that pay us millions and millions of dollars a year all the way down to thousands of dollars a year. And the reason for that is our platform and our technology scales, but cyber attacks don't discriminate. They do not discriminate based on size of organization, industry, or location. They are broad these days. The volume continues to increase, sophistication continues to increase, and everybody's a target. And over the last several years, that's matured into everybody being a potential customer and keeping us very busy.

Jarrett Banks: Okay. Turning back to Adam, what does the market opportunity look like for external cybersecurity in the future?

Adam Gerchen: Well, I'll let Foster, the industry expert, offer up his significantly more learned opinion than mine on what's to come in this market. But I would just say more broadly, as an industry and why we found it intriguing, we've always been attracted to cyber as a sector because of how much it touches all the areas of focus I just enumerated. Large enterprises, small and medium-sized businesses, multinational financial services firms and fintech startups, public sector clients all have to focus on cyber threats as a core component of having strong compliance, regulatory or governance regimes. And if they don't, they obviously face material legal risks.

So it really does cover all the components of our GRC and legal focus, the lines between which, as we've said before, continue to blur. And cyber, I think, squarely hits on the drivers of the investment thesis I mentioned earlier. The world is only getting more complex and risky because of digital proliferation. So we love the macro tailwinds. And I would just add, drilling down just a little deeper, we have always observed how public markets and cyber have rewarded category champions, but the categories of important shift as technology develops and adversaries evolve. So it's somewhat unquestioned that the next frontier is external, the threats that exist outside of the firewall, and ZeroFOX combined with IDX is dominant in that category.

Jarrett Banks: Okay. Foster, you want to add to that?

James Foster: I think that was a pretty good job. I'll maybe come at it from just a slightly different angle. And in cybersecurity, the staying power of a category champion, just playing off what Adam said on the category champions, really is predicated on the size of problem you address for customers and the amount of pain that you solve for them. And so I go to bed sleeping well every night, knowing that I'm working on a bigger problem tomorrow than I did today. There are more external attacks. Those attacks, like I said before, are increasing in volume and sophistication, and they're going after new types of customers.

10, 15 years ago, the primary target for organizations was financial services organizations and maybe government. And you went after financial services organizations because you wanted money, or you went after the government because you wanted maybe intellectual property, information, something that could give you a nation state competitive advantage.

But today, everybody can be a target. Ransomware has really leveled the playing field where I could hit an organization that could be a small school district and charge them $10,000 to get access back to their systems, or I could hit something bigger and charge them a half a million dollars or even $10 million and everything in between.

And so the financial gains, the return on investment, if you will, for these cybercriminal groups continues to increase year over year, creating more problems. And when there's more problems, people are willing to spend more to protect their organizations for those problems. And I don't see any trend in our business or even in the sector right now that says there's going to be fewer problems in the near term than we have today. And so I think that sets up cybersecurity to continue to be a relevant sector at the boardroom level.

Jarrett Banks: Okay. Certainly food for thought there. Sticking with you, Foster. How are you guys different from some of the well-known industry players like CrowdStrike and Zscaler?

James Foster: Well, Jared, I take offense. I would say that we're well-known in our sector. Look, I think cybersecurity may be unlike some areas of IT, where you've got a winner take all and productivity software like Microsoft has had for decades, and maybe operating systems. Cybersecurity, you have best breed providers that offer their technology, their platforms to solve, again, particular pain.

CrowdStrike and SentinelOne are the new market leaders, and they do a really nice job of protecting devices with their agents. But if you ask them to use their technology to help separate the in from the out, they wouldn't come close to providing the same value that a Palo Alto capital networks or Zscaler could provide. And there's different tactics that the adversaries and attackers of the world have used to target and get into organizations. And so, unfortunately for the better part of two decades now, enterprise organizations have followed U.S. military theory and the kind of trainings they had, which was a defense in-depth strategy. Works, and it works not only in practice in the theory, but in the field.

And so, pick your best of breed providers to protect the things that they need and make sure that you've got a defense in-depth strategy across security, which typically means that you'll have a handful of trusted partners. I believe ZeroFox is in that handful of trusted partners to our customers. We are an important part of that tech stack now, and it continues to prove out in terms of size and scale of the business, and size and scale of the problem that we're addressing.

Jarrett Banks: Great. Now, I want to bring Tim back into the mix here. I can see that your enterprise customer business is growing at a nice clip. What can you tell me about your customer mix and how it's changing, and then just as a follow-up, what would you say is your most important growth area at the moment?

Tim Bender: Yeah. Thanks, Jared. First, our customer base ranges from some of the largest corporations in the world, including several of the Fortune 10 to SMBs. However, what we've experienced in the past several years as it relates to our mix is an increase in larger entities adopting our solutions. So for example, over the past three years, the number of customers that pay us in excess of 100,000 per year has grown at a 50% annual clip. So, we're really pleased with that growth. As that relates to overall growth, we see that continued adoption by those larger entities, such as the Fortune 500 or Global 2000 as an important growth area for us. We're less than 10% penetrated in that cohort now, so we see a lot of opportunity within those entities.

Another area for growth that we see is within our own existing customer base. We have a lot of white space there, and our ability to upsell into that base will be an important growth driver for us as well.

And then finally within the growth story, acquisitions or inorganic growth is really important to us. We completed two acquisitions in the past, let's say year and a half, and concurrent with our merger with L&F, we will acquire IDX and we'll talk about that a little bit later, too. So, inorganic growth is very important to us.

Jarrett Banks: Great. And then just, Tim, sticking with you, I'm sure you get this question a lot as a CFO. Can you talk about the opportunity to expand margins over time?

Tim Bender: Sure, absolutely. So, first. Historically, we have a demonstrated pattern of expanding our margins over time. And then as we think about margin on a perspective basis, we look at it from two lenses. First, on the revenue side. As the market for external cybersecurity has matured, and our customer requirements have grown over time, the value for our services has grown as well with that. So, we see contribution from the revenue side. From the cost side, and then I'll go back to the video that you saw, that was our platform. We've invested heavily in our platform over time, and we'll continue to invest in R&D to expand our platform and basically improve our capabilities as it relates to our ability to collect, ingest, analyze data, as it relates to our customer's problem set. And because of that, I think we feel confident we can expand margins over time.

Jarrett Banks: Great. Okay. Foster, let's get into that IDX deal. As mentioned, the SPAC structure allows you to give pro forma numbers. What kind of synergies do you expect?

James Foster: Look, we're a growth organization, so I think we are focused more on what I call revenue synergies as opposed to cost synergies. This is not a roll up, cut cost, and try to squeeze every penny out of the organization that you'd see maybe in different strategies. Our strategy is a growth organization. You've seen that historically from both organizations, and you'll see it in our projections that we put forth, that we continue to believe that we've got a really interesting opportunity for organic and inorganic, as Tim mentioned, growth in the near-term and long-term.

What we'll see out of the gate, which was disclosed here, is IDX in general is a U.S. based business. ZeroFox is a global organization. We've got customers in 50 countries. We've got teams around the world. Half of our employee base is, in general, outside of the United States of America. And so, we think we bring great distribution and scale to the relationship on day one with a global customer base and distribution channel set.

Outside of that, we also believe the combination of our platforms will be interesting. The IDX customer base in general is responsive. They are world class in their capabilities around breach response. It allows them to be very quick to respond in the case of a breach, and be there to be that trusted advisor, right? I got to say one back to pat, one throat to choke. And ZeroFox coming in will help take that customer that needs breach response and can offer protection capabilities to make sure that breach doesn't happen again, and we think that'll be a really powerful value proposition for our combined customer base, and it's something that we've had the opportunity of working on together for quite some time now.

I don't think I've ever done an acquisition in the course of my career where I've had, in general, a year to plan for it. And so, I couldn't be more excited about what Tom Kelly and his team has done at IDX and what we're about to accomplish as a combined company here shortly.

Jarrett Banks: Great, and I would just recommend to our viewers to check out the investor presentation on the ZeroFox website if you want to know more about the IDX deal and some synergies there. Foster, sticking with you. Can you talk about IDX's customers and how the deal allows you to bring in a more diverse set of clients, and does that also include government entities?

James Foster: Yeah, it does. I mean, we both have public sector clients. We both serve enterprise quality clients. I think part of the difference here is there are broader groups of customers that are coming into IDX on a responsive basis, or a reactive basis, where a lot of what ZeroFox sell is protective capabilities to make sure customers do not get targeted, attacked, and breached.

And so, we take pride in making sure that, once a customer implements ZeroFOX, that they can sleep a little bit safely, more safely at night and have a better peace of mind. And I think we'll have the opportunity to show that same value to the combined customer base, take those customers where there's been an unfortunate incident, get them through their regulatory requirements as fast as possible, and then start working on protecting that organization so it doesn't happen again.

And as you saw, you just mentioned in our investor deck that's out there, you'll see a real value proposition and it takes you from response to protection very, very quickly. And that race condition, that window of time is what I will be laser focused on as an organization when we come together; helping customers go from breached to protected and as fast as possible. That's the race condition that I want customers holding us accountable for.

Jarrett Banks: Okay. Now, you may have a unique window into this next topic: Ukraine. Of course, everyone is aware of what's happening. Has ZeroFox been monitoring the situation? What are you seeing?

James Foster: We have been. We've been publishing threat intelligence on this. We've got a global threat intelligence capability. As a recap for our platform, we suck in tremendous amounts of data: everything from open, deep, and dark web, social media, mobile app stores, and then areas that are hard to get to in deep and dark web forms. We pull all this data into our platform, and turn it into actionable threat intelligence for our customers to where we can leverage the platform to take action on their behalf, or get it in the fingertips of their analysts as fast as humanly possible.

This conflict that's happened in Russia and Ukraine right now has created a lot of volatility for our customers. And in general, nobody is safe. Organizations that have decided to maybe align themselves with Russia or continue to operate in Russia, maybe they're not necessarily Putin advocates, but they continue to operate businesses there; are being targeted now by anybody that is against Russia. And so, they've seen heightened risk profiles for organizations that maybe continuing to operate businesses in Russia.

At the same time, anybody that is supporting Ukraine around the world has got heightened risk profiles for some of the nation states that are out there that are supporting Russia's efforts. And so, unfortunately that's left the enterprise world in Western Europe and throughout North America, even Southeast Asia, as the crosshairs of one or the other for just everybody. And so, unfortunately there's no safe spot anymore, and I think this heightened volatility and conflict will draw out, and it will lead to increased cybersecurity awareness. I don't talk to a customer at all anymore that feels safer this year than last.

In the world of COVID, you had increased cybersecurity risk because of so much digital transformation that was taking place and changes in the workforce and how work was getting done. And now, you have heightened cybersecurity risk because there's a cyber cold war happening, and everybody has fear of being attacked as a part of a retaliation. And given that there's a no safe space, it's creating some real productive paranoia and spend and making sure their strategies are the right ones.

And I think the long-term effect of all of this is, I think cybersecurity as a risk area will continue to grow, but you'll see it shift in cycles. We're going to be on a cyber war cycle now for probably the next couple years, and TBD what the next cycle after that is. It's an interesting market to navigate for sure, and unfortunately.

Jarrett Banks: Certainly. Certainly something to keep an eye on. Absolutely. Tim, maybe just switching gears here, let's talk about M&A. Is there room for more consolidation in your sector that you've identified targets already?

Tim Bender: Certainly, and one of the reasons we're doing this transaction is to be acquisitive. So, we've already stated that as one of our growth strategies. There are certainly targets out there. Have we identified them? I mean, we're not going to go into details now, but Foster is generally and routinely going through a list of targets. There's definitely more room for consolidation in this market.

Jarrett Banks: Foster, your thoughts on M&A?

James Foster: I think I heard it that there's roughly... There's over 1000 private cybersecurity companies around the world today. There's roughly two dozen, depending on how you count the list, that are publicly traded. And so, if you want to think about riding the wave as a public organization, you've got two dozen surfers in the ocean and 1000 people watching. I think there's a lot of opportunity for consolidation, and I think there's a lot of innovators out there that maybe haven't hit scale. Maybe they don't have the full picture of the pie. They may be building really great tech, but have challenges in getting a go-to-market engine correct.

I think as we continue to scale as an organization, we'll bring not only pace of innovation as a competitive differentiator to us when we're thinking about acquisition targets, but also scale and distribution, scale and customer satisfaction, and it's a broader platform and capability set.

We are constantly looking, constantly evaluating, but make no mistake; our bar for acquisition targets is incredibly high. Starts with people. You've got to have the right people that are passionate about their business and passionate about delivering value to their customers, and then you've got to have some really interesting trade craft or intellectual property to go along with that. There are very few companies that pass the people test. Find great world class talent is always a challenge, and we hold our bar hard for a reason. Our customers expect it.

Jarrett Banks: Okay. Foster or Tim, will the proceeds from the deal mainly go to organic growth, or is some set aside for M&A?

James Foster: I would say, in general, we have the capital we need to operate this business for years to come. The M&A, because we don't have a particular M&A target in mind post-IDX, that could vary. I mean, it could vary in size, scale. And I think what's probably important here, and something that Adam certainly can speak to as well; being in the capital markets, being a publicly traded company gives us additional dials to go after and make sure that we're evaluating a different class, maybe, of target than we could have evaluated as a private company. And we'll have more opportunities for capital, whether that's through equity, cash, debt offerings, or even some performance targets as well. We'll have lots of different dials to choose from. And I have confidence that we find the right company, we'll figure out the capital requirements and how to get there secondary.

Jarrett Banks: Great. Okay. I see the questions are coming in. We do encourage everyone to ask questions there in the Q&A, and we will ask them live. Gentlemen, this is a good point for me to pass the baton over to my colleague, John Jannarone. John, take it away.

John Jannarone: All right. Thanks a lot, Jared. I do see some questions coming in and we're going to get to those, but we got a few more points I want to touch on here. Foster, I think that something I notice going through your presentation is just a rainbow of different companies, dozens of names that I recognize as clients. Explain something for our audience, are you pretty much industry indifferent? I mean, I see banks, automakers, et cetera on there. Do they all really have cybersecurity risks and therefore it's not really sector focused, but it's you have something for virtually everyone?

James Foster: We do, for better or worse. Again, I think we will offer protective capabilities. The way that our platform is set up can scale up or down to the largest organizations in the world. As Tim mentioned, we have multiple companies that are in the Fortune 10. And so we've scaled all the way up stack to companies that are down in the SMB space paying thousands of dollars a year and everything in between. And I think that proves that we've built a platform that can scale and can scale well, but it also proves that the market and the TAM are going after is pretty large in size. It's not just a particular vertical, it's not just a particular company size or scale that is the ideal customer for ZeroFox it's in general anybody that operates in the new digital world we can add value to and is unfortunately also a target. And I think that just gives us lots of time to continue to grow into that TAM.

John Jannarone: All right, great. I'm going to sprinkle in some of the questions that have come in and then we'll get back to some of the other ones that we wanted to ask you. Foster, Namal here is asking how do companies look at what their budget should be for cybersecurity protection? Is it a fixed percentage of revenue or what's an appropriate amount to spend the adequately safe?

James Foster: Look, it is different depending on the type of company. So I will caveat the answer with that it's different depending on the sector that you're in and the risk profile of an organization. For example, a regulated industry may spend more on cybersecurity compliance related activities than an unregulated industry. An industry that has a higher target profile, such as financial services, next generation digital technology, they may spend more on a per capita basis as well. However, most of the times what we see is cybersecurity is budgeted as a percentage of IT spend and IT spend is budgeted as a percentage of maybe total revenue or total expense. And in general, we see cybersecurity in that mid to high single digit ratio of total IT spend. And in certain organizations, it is common now to see cybersecurity being in that double digit range as well. Again, when it's mission critical.

And I'll give you maybe one or two examples of what I mean by mission critical. I mean a digital company that comes out now that doesn't have any office space that has 100% remote workforce that's reaching their customers through digital means only. If those digital channels and brands and assets they have have been compromised, it could cost them everything. It could cost them a day, a week, or maybe even a month's worth of value or revenue and that could be the difference maker for that organization. And so we see those kind of organizations that are digital first and maybe even digital only spinning ahead of their peers, realizing that they're protecting their crown jewels, their digital assets.

John Jannarone: That's a great answer. Foster, I'd like, if I could, ask you to talk just for a couple of minutes about your AI, for those people who are interested in a bit of the mechanics of how that works.

James Foster: Sure, yeah. So we've invested heavily in artificial intelligence. We've been doing it for several years. I think we even announced it back in 2019. Part of our partnership with Intel with was part of their AI builders program. It's something that we had spent years on before that announcement working with them and others and that allowed us to build a platform to scale. And maybe just one or two examples to make this more real. For example, when I say that I consume digital data and I mine that digital data for intelligence, I'm separating signal from noise. And in order to do that, you have to use artificial intelligence now, but it's not just a marketing buzzword, there's multiple different variations of AI to potentially implement and use for the problem set.

For example, if I wanted to use AI to determine if some textual content that I was consuming was bad or good, was angry or happy, you could use an NLP, or a natural language processing engine, to help determine the sentiment or maybe even the language of data that you are consuming and you can apply those results into your analysis or into your engine for determining what to do next. There's a whole different breed of AI that we've leveraged to do image analysis. This is called computer vision. That allows you to deconstruct pictures, video, maybe even sound and pull it apart to actually get contextual analysis at a deeper level. We use this internally for image analysis. It's a great example of how you may be able to identify images within images. Maybe it's a logo within an image. Somebody that's using that logo to fraudulently attack someone's brand or maybe even use it to create phishing pages around the world on social media platforms or on web platforms to go after an organization and target their employees or customers.

In any case, you have to be able to use an AI library like this to identify the picture to say, “Is this a picture yes or no?” To identify if there was a picture within a picture for a logo, for instance, it would be a yes or no again. And then you would apply that with a bunch of other algorithms that we have to determine to say, “Is this malicious or is this safe?” And so again, without AI at scale, none of this would be possible. The old way of doing this was to apply a tremendous amount of people and human analyst talent to look at things as efficiently as possible to go, “Yes, this is bad. No, this is good.” And that just doesn’t work anymore in the amount of data that’s out there, especially external data that we consume. And we’ve gotten dozens of patents out there in our name, we constantly work on more and we’re constantly pushing the envelope here for pace of innovation and in particular AI innovation.

John Jannarone: That’s great. A question for you about a shift that I’m sure everyone’s aware of. So as more activity moves to the cloud, does that increase the frequency or the risk of cyber attacks?

James Foster: Look, I don’t think it actually increases the risk of cyber attacks per se, but it changes the tactics. And so when you take an asset class, even if it’s just multiple servers maybe that were in DMZs inside of organizations and push them to the cloud or push some of your internal computing to the cloud, you have just different assets, which means that they can be attacked differently. And it doesn’t necessarily mean that they will be attacked more, but the success of those attacks may actually increase. And I’ll explain that here. And so when you adopt a new technology in general in cybersecurity, you’ll see the conversion ratio or the likelihood of success of attack go up for a period of time because security lags IT. And so there’s a new IT trend that’s out there, everybody starts adopting it, security products that typically bolt on around it take time to develop and innovate and deploy.

And so you’ve got this window of vulnerability between the adoption of new technology and then the securing of it. Organizations still miss the basics. They adopt these new projects, they have aggressive digital transformation timelines, and security is sometimes one of the things that continues to get cut, something gets compromised, everybody goes into this reactive state and says, “We should have spent more time securing this while we were building it as opposed to after the fact,” and now you’re doing cleanup. And that cleanup is a great example of why IDX is in business, they provide breach response capabilities. And why ZeroFox continues to grow is that there are more assets out there for us to protect. And like I said, it’s keeping us busy.

John Jannarone: Now I know you've already done a great job of explaining what's behind the increased risks and activity, but I just want to cite a number here from Forester, not Foster that 63% of organizations were breached in the last year. That number is just mind blowing I think to a lot of people who are not familiar with this industry. Can you tell us a little bit more about what's going on there and is it going to go higher? It sounds like it might, you're talking about it getting more scary out there by the day, not feeling more comfortable.

James Foster: Well I could flip the coin for you. 100% of organizations were attacked last year, 100%. Great news, and only 63% of them maybe got through. And there's some number in between 63 and 100 that got through it, they just don't know it yet. And so I would say the shocking number should always be that everyone's being attacked and very little ramification, there's very little we can do as a country right now to stop that. And that's something that we've got to get right on and we've got to get fixed. And not only as a country, but as a society around the world. Cyber attacks can't cause havoc to any kind of organization around the world forever. And the playing field is not level.

In general, even the best organizations and the biggest organizations in the world that have really sophisticated apparatus and teams and resources to combat this, they're still not combating another organization. They're combating a country's cyber adversary. They're going against somebody's military. It's not a fair fight, it will never be a fair fight and so the only way to do that is to change the game and change the paradigm here, something that we're hoping to help do.

John Jannarone: Great, now Foster, I promise we're going to come back to you, but I want to rope Adam back in for a moment if I can. Foster's done a fantastic job explaining the business and he is the expert, and we're actually going to talk to him more about his background momentarily. But Adam, can you tell us, what's your role going to be after the deal closes? Will you be an advisor? Will you be on the board? Where do you see yourself participating?

Adam Gerchen: Yeah, well I'm proud to be joining the board of directors. So I'll aim to help Foster and broader team in whatever way is needed or welcomed. But regardless from our very first meeting, I told Foster that I had one goal, which is to see the continued success of the ZeroFox platform as it transitions from private to public markets. So formal or informal, titled or untitled, we're strategically and economically aligned. So whatever he and the team needs, they're going to get. Where I think we've identified the most value add to date is actually on the BD side. So driving some new client verticals, be it further into fintech, law firms, and the legal ecosystem more broadly, et cetera.

John Jannarone: Great, I'm going to drop in another question that I just saw pop up here. Is digital currency a new front in cybersecurity? It's not being used to pay for goods and services too much yet, but is it on the horizon and is that on the way? I'm not sure who wants to take that, Adam or Foster?

James Foster: Look, I'll take it. It's an asset class and in particular it's a digital asset class. And whether it's NFTs, which people still have trouble wrapping their head around, or digital currencies out there, different kinds of coins that are out there, whether it's digital coupons for services, products, or goods on different sites, ad campaigns, all of these things now are digital value systems. And those digital value systems can be attacked and fraud can be rampant in there to the scale we've never seen before. I have brick and mortar business customers that are constantly being targeted with what I call digital fraud, people selling fake coupons for them as an example. 50% off for $10, $20 gift card for $5. And they get to these stores and try to use them and those companies, they don't work.

And this isn't real. And so it's very hard to differentiate fraud in the digital realm between something that's legitimate, creating a digital brand and identity for fraudulent use is easier now to do than ever. It's cost effective. And whether, again, financial gain is your target, which is where we see a lot of fraud and financial targets, or whether it's stealing information, getting a competitive advantage, going after nation state secrets, you could use the same exact tactic to get back the different type of result. Again, money, information, or competitive advantage. It's all the same, basically.

John Jannarone: Great. Foster, you talked before about when you're considering an M&A target, the importance of having the right talent at that company. Can you tell us, how does the industry feel when you're looking at organic growth, are there enough talented people out there to join this company who are talented enough to know how to continue to develop the AI and do everything else you need? This seems like a pretty specialized skillset.

James Foster: I'm not sure there's enough talent right now in the United States to solve all the open jobs that are out there. But I think in general, cybersecurity has a 0% unemployment rate for a decade now. And so no, I think there's a talent shortage not only in North America cybersecurity talent requirements, but our global talent requirements. Finding great people, regardless of industry, is always a challenge for any successful company. And any CEO that doesn't put that as a constant challenge and a constant place to invest in your people, I think is missing the mark. A lot of people ask what our greatest asset is and I think they would expect us to say our platform or our AI. Our greatest asset at ZeroFox, to be very clear, is our people. It's our longest competitive advantage.

It's something that we spend the majority of our money on and our investment. If you look at our cost bases of an organization, we're a people intense business that builds our product. And so we'll always invest in them. And we invest around the world. Like I said, we've got more than half of our employees now, roughly speaking, outside the United States. And so we've found really interesting passionate talent bases around the world and we'll invest in them just like we invest in those talent pools here in the United States. And we're a global company and we'll act as such in the years to come.

John Jannarone: Great, and I'm sure that anyone who's listening can tell that Foster has a ton of experience in this industry, but in particular Foster, you founded and sold a company. Can you tell us a bit about what you've seen over the last couple decades? How that helps you guide this business and are you surprised by where things are now compared to when 15 years ago, the way world was very different in terms of cybersecurity. Have things played out as expected, or have you been surprised?

James Foster: There's a few surprises. I remember working for the federal government here in the late '90s, and then when Y2K didn't blow up the world, I transitioned into the private space here in January of 2000, literally January of 2000. I moved from Boston to New York to California, and did startups that were acquired by McAfee, Verisign, and KKR. And I remember the pitches 20 plus years ago saying, "Oh, things are going to get worse, attacks are going to get more complex, you need to protect yourself." We say the same thing today, and it's not snake oil, it just continues to be surprisingly true. There's always more attacks and I think part of this is going to work its way into a long term fundamental position that the cost of an attack will continue to come down over time. Therefore, by design, when the cost of an attack goes down, the number of attacks will go up and your success ratio for those attacks can also decline over time as well. And so I think that's something that organizations are seeing firsthand. It's something I've experienced in my career. I continue to wake up and see if there's a year that I'm like, "Great news. Cybersecurity has figured itself out." But I've been doing this almost 25 years now and it hasn't happened, for better or worse.

John Jannarone: All right. Let's let Tim chime in for a minute. We just heard from Adam talking about how one advantage he sees having is helping bring in new clients, but how do the numbers look there, Tim? I mean, have customer acquisition costs gone down? Can they go down further? How does that play out as the company continues to scale?

Tim Bender: Sure. And, listen, I've been here for six years, started out very early when external cybersecurity wasn't a tagline we were using. This was a very nascent market. So we were fighting hard for every sale that we got. As we've matured and as the market matured, we've certainly seen our customer acquisition costs come down. We've seen our average revenue per customer, our average selling price, almost double in that same timeframe. And then we've seen the productivity from our sales reps nearly double as well as quotas have gone up. So all those contribute to an improved CAC, and then with our strong gross margins and our strong net retention rates, certainly, our customer acquisition costs have come down and our LTB to CAC ratios certainly align with the broader SaaS industry.

John Jannarone: Great.

James Foster: There's a number behind that too, John, that I just want to double click on there, which is the number of things we protect for organizations has doubled as well. And so the quality of assets that continue to create themselves beyond that traditional firewall goes up, it continues to increase, and they continue to rely on ZeroFOX for that next innovation and protecting that next investment. And so that's very important to our core business as well, being there to help our customers protect what's next, not just what they have today.

John Jannarone: Great. And, Foster, we've talked a bit about these very, very large clients you have, but I just want to make clear, the way the model's set up, you can very easily serve in a profitable way much smaller clients if you find them. You talked about the SMBs. Is that right?

James Foster: We do. We serve small, medium, and large customers, private and public and everything in between.

John Jannarone: Foster, we've talked about M&A quite a bit. The IDX deal is pretty transformational. When we think about M&A, is there scope for something else of that size that could really change the face of the company or are you thinking more bolt-on stuff in the next few years?

James Foster: Look, I think we'll have the opportunity to do both. I think there's a really interesting opportunity to continue to do what I call transformative M&A, but, again, the bar is high and we have to find the right organization. We don't need that as an organization or as a business to be successful. We've got a successful platform today, capabilities, and a really nice growth trajectory. But if we find the right type of opportunity to add world class talent, revenue, and intellectual property into the mix, we'll look at it.

I don't think there's necessarily an organization that would necessarily be too small for us to look at, and so we'll have to make sure we say no quickly. I think that's the guidance I continue to give my team. There's hundreds and hundreds of companies out there with their hands up saying, "I would love to be acquired," and you don't have time in the day to talk to all of them. We have our strategic areas of interest. We look at those, we get to know the teams, and you move slowly in that world. These are big decisions to be made.

John Jannarone: Great. And this is a bit of a fun one. You talked about NFTs and this digital asset class, but another thing we hear about all the time is the Metaverse. Does the Metaverse present any cybersecurity risks or is it too early to start thinking about that?

James Foster: No. We already published a research paper on that, actually. I think Metaverses pose a very real risk to organizations. Our view here is it's a replay of about 25 years ago when the web was created. There were companies in the early days of the web, if you were operating the dot com boom it's, "Oh, we don't need that. We have stores. We don't need the web. That's not here for the longterm." I think, as we'll see, probably in another couple decades from now, Metaverses are here for the longterm. They are very, very real and the security risks that come with them will certainly be vast and complex as well. But it'll take time to play out. I mean, you've got to create the Metaverses first. You've got to get engagement. You've got to get real time adoption. And then once those things happen, then attacks will happen behind it, guaranteed. Attacks happen where people and money are. You just follow people and money and you'll find cyber problems.

John Jannarone: Great. Something that we talk about both here on IPO Edge and our sister platform CorpGov is insurance. While not the sexiest topic, it gets a lot of attention right now because it's expensive. I've got to imagine that cyber risk has got to be a part of what people are worried about. How do you fit into that story? I mean, do people need to buy insurance or are they just perhaps buying help from companies like yours? How does that all shake out?

James Foster: Look, I think when I talk to CISOs, Chief Information Security Officers, cyber insurance is becoming one of the strategies that they deploy as a part of their defense in depth strategy again. And some spend more on insurance and less on protection. Others spend more on protection, less on insurance. I'm not sure there's necessarily what I'd call agreed upon best practice today on what level of insurance you should have as a percentage to your spend in cybersecurity. But I think that'll get worked out over the next five to 10 years. And, in general, you've got premiums that will start to normalize. You'll have tech stack requirements that'll start to normalize, because the insurance companies just can't come in and insure everybody at very low premiums and then offer a lot of value when something bad happens.

And if there's an increase like there has been the last couple years to continue attacks on organizations, it's going to be counterproductive. I mean, if every company's being targeted and every company was insured, you won't have that industry. If every house was burning down every two years, you wouldn't have fire insurance. That wouldn't be an offering. So we've got to get to a normalized state here in the coming years for sure.

John Jannarone: Great. A question here is, how quickly can someone get the protections that you would recommend in place? I mean, I imagine that, as is often the story, people wait until something bad happens. Once someone's in that boat, how quickly can you get them into the shape they need to be?

James Foster: Minutes.

John Jannarone: Wow.

James Foster: Minutes. We could turn you on and get you protected in minutes. As you saw in that video in the very early part, our response time is measured in seconds. Protection and time to value can be measured certainly in minutes. We're there to help. And, unfortunately, that's the expectation in cybersecurity. This is not a six-month deployment cycle that needs lots of planning out. You need to have the ability to be nimble. You need to be able to start with something, and then if it is a large enterprise wide deployment, that's fine. But, again, I don't have a single customer that said, "Hey, this is great. We'll spend the next six month deploying this." The expectation is time to protection, time to value is very, very short in cybersecurity and always has been.

John Jannarone: Great. Another topic that, of course, has been in the news nonstop the last year or so is the supply chain. I think some of that may have to do with cyber attacks, not sure, but is that something you discuss with your customers, protecting their supply chain?

James Foster: We see it all the time and we have supply chain intelligence capabilities that we provide to our enterprise customers around the world, especially those that are in manufacturing or have more robust supply chains that they depend on. And they depend on our intelligence to make sure that those supply chains are not disrupted or if they are going to be disrupted that they have upfront intel around that and ways to maybe de-risk their own businesses. And so I think they've got real value out of ZeroFOX's supply chain intelligence capabilities.

With that said, the supply chain and what's happened over the last couple years has affected some of our customer cohorts and I think intelligence as a way to help de-risk their business has been very valuable. The situation in Ukraine and Russia has disrupted supply chain to a smaller extent in the global sphere. It's still just what I'd call the COVID tail, and I expect that there will be supply chain disruptions for the next couple years minimum.

John Jannarone: Great. You talked before about this immense amount of data which is just unmanageable without the help of some AI, but I'm curious, we've had a number of companies come on our program here who are collecting or organizing satellite data and there's proliferation of this industry in space. Is that part of the story here too, keeping track from way up in outer space? Do companies rely on that sort of data? Is it an important part of the cybersecurity story?

James Foster: Look, I think it's new comings there. I think there's a lot of innovation that needs to happen. I'm not sure I know of any material cybersecurity space providers yet. Maybe I'd volunteer for that job right now if that got me to space. So TBD on our space offering that we'll launch sometime later this year, if we get a free ride from Bezos or Musk. I think maybe what's more interesting here, if you want to branch off, is that Musk just acquired Twitter. Everybody saw the news here in the last 24 hours. It seems like they've got an agreement. Maybe one of the things that he hasn't recognized yet is, not only is he acquiring a social platform or the town squares, he recognizes that, he's also acquiring a battlefield.

Twitter is a battlefield and we had reports as early as 2015 that showed how Twitter, as an example platform, was being used by nation states around the world to target other governments. I'm not talking about targeting politicians. I'm talking about targeting employees and targeting key personnel as a means to get to an end. And I think there's a lot of work that will become more and more relevant. When I talk about digital asset protection and social media protection, Twitter is one of those platforms that commonly gets exploited and abused by agitators around the world. And so I think we welcome Musk's involvement here, and welcome to cybersecurity. Should be a [crosstalk].

John Jannarone: I'm glad you brought that up, Foster. I mean, I've got to ask as a follow-on there, I think there are some companies that discourage or even forbid their employees from having social media accounts. Is that a way in the back door, in some cases, where an account gets hijacked? Tell us a little bit about how that works.

James Foster: I think it's comical. Any CISO that's out there that said, "Oh, our approach to this is to disallow employees on social media," that doesn't work. It's not a practical policy or position. So anybody that's hearing me now that says, "Oh, that's our policy," I'm telling you, it doesn't work well. I have talked to CISOs. Typically, several years ago that said, "Oh, by the way, we block LinkedIn or we block Facebook or we block the web." And I'm like, "Well, you might as well cut off the internet. I mean, I don't understand what your people do in terms of research then if you don't have some of these platforms." They're platforms for business. They're platforms for engagement. You'll be at a competitive disadvantage if you aren't adopting new platforms and technology right now. And so I don't know any successful business that's cutting off their digital legs as a part of their growth drivers.

And so the right policy and the right approach to this is, adopt these technologies, be thoughtful when you do, bake security into the program out of the gate, and do it the right way. Don't turn a blind eye and just say, "We don't allow this," because what will happen is they'll go create what we call fake Instagram accounts and fake name accounts and still engage. And they'll think they'll be sly about it, but all of a sudden, somebody'll pick up a company logo in a shirt they're wearing. The adversary will use the same type of AI we use to go looking for employees and they'll become targets. That's a real tactic that's being leveraged today.

John Jannarone: Great. I just want to sneak one more in, because we're almost out of time here, then I'm going to let you have the last word as well, Foster. But we talked about your international footprint, the number of your staff who are outside of our borders. Do you see much more opportunity to keep growing internationally or is the focus more in the U.S. going forward? And also, is it harder to offer your services in some countries? Do you have to change the structure or anything like that or is it universal enough?

James Foster: Well, my General Counsel is not on this call. I would tell you it's not hard to do that. And then he would sit next to me and go, "It is hard and I take care of that." And so, look, I think gaining experience and expertise around the world and becoming a global company is not easy. I remember the early days of ZeroFOX when we were operating in and around Washington D.C. primarily, and first getting to Canada, then getting over to the United Kingdom, then starting to move beyond those steps, it took real time. And then making sure that you're breeding culture and you're creating culture champions in those regions around the world that respect local culture, but then bring in broad company culture and tie that around the world into some common themes and some common values that we believe in as an organization.

It's not easy to do and there's very few one on one books that you could read to do this. And so our go-to continues to be people. I say it all the time, you want to build a great culture, don't offer free granola bars and time off. Hire the right people that are passionate about what they do, and that's the number one thing you can do to build the right culture. We will continue to invest everywhere in the world that we think makes sense. Certainly, outside of the United States. We'll continue to grow our teams that we have right now and we're constantly evaluating what the next center of excellence will be for ZeroFOX as a part of our global expansion plans.

John Jannarone: All right, great. We're going to have to leave it there. I'm just going to remind everyone, if you'd like to watch a replay, it'll be up within an hour or so on IPO-edge.com. Or you can just go look up the ticker, LNFA, for the SPAC, which, of course, will change to a new ticker after the deal closes sometime later this year, I believe. Thank you, gentlemen, all three of you, for being here. Everyone who joined and asked questions, we really enjoyed it. Hope to see everyone again soon.

James Foster: Thanks, everybody. Have a great day. Thanks, John.

Forward-Looking Statements
Certain statements in this communication are "forward-looking statements" within the meaning of the "safe harbor" provisions of the United States Private Securities Litigation Reform Act of 1995. When used in this report, words such as "may", "should", "expect", "intend", "will", "estimate", "anticipate", "believe", "predict", "potential" or "continue", or variations of these words or similar expressions (or the negative versions of such words or expressions) are intended to identify forward-looking statements.

These forward-looking statements and factors that may cause actual results to differ materially from current expectations include, but are not limited to: the inability of the parties to complete the transactions contemplated by the definitive agreement relating to the business combination and other transactions that will result in ZeroFox, Inc. ("ZeroFox") becoming a publicly traded company as ZeroFox Holdings, Inc. (the "Business Combination"); the outcome of any legal proceedings that may be instituted against L&F Acquisition Corp. ("LNFA"), the combined company or others following the announcement of the Business Combination and any definitive agreements with respect thereto; the inability to complete the Business Combination due to the failure to obtain approval of the shareholders of LNFA, to obtain financing to complete the Business Combination or to satisfy other conditions to closing; changes to the proposed structure of the Business Combination that may be required or appropriate as a result of applicable laws or regulations or as a condition to obtaining regulatory approval of the Business Combination; the risk that the Business Combination disrupts current plans and operations of LNFA, ZeroFox, ID Experts Holdings, Inc. ("IDX") or the combined company as a result of the announcement and consummation of the Business Combination; the ability to recognize the anticipated benefits of the Business Combination, which may be affected by, among other things, competition, the ability of the combined company to grow and manage growth profitably, maintain relationships with customers and suppliers and retain its management and key employees; costs related to the Business Combination; changes in applicable laws or regulations; the possibility that LNFA, ZeroFox, IDX or the combined company may be adversely affected by other economic, business, and/or competitive factors; LNFA's, ZeroFox's or IDX's estimates of expenses and profitability; expectations with respect to future operating and financial performance and growth, including the timing of the completion of the proposed Business Combination; ZeroFox's and IDX's ability to execute on their business plans and strategy; the ability to meet the listing standards of the listing exchange on which the combined company will be listed following the consummation of the transactions completed by the Business Combination; and other risks and uncertainties described from time to time in filings with the U.S. Securities and Exchange Commission (the "SEC").

You should carefully consider the foregoing factors and the other risks and uncertainties described in the "Risk Factors" section of LNFA's registration statement on Form S-4 (File No. 333-262570) and amendments thereto filed in connection with the Business Combination, and other documents filed by LNFA from time to time with the SEC.

Readers are cautioned not to place undue reliance upon any forward-looking statements, which only speak as of the date made. LNFA, ZeroFox and IDX expressly disclaim any obligations or undertaking to release publicly any updates or revisions to any forward-looking statements contained herein to reflect any change in the expectations of LNFA, ZeroFox or IDX with respect thereto or any change in events, conditions or circumstances on which any statement is based.

Additional Information about the Business Combination and Where to Find It
LNFA has filed with the SEC a Registration Statement on Form S-4 (as amended or supplemented through the date hereof, the "Registration Statement"), which includes a preliminary proxy statement/prospectus of LNFA, which will be both the proxy statement to be distributed to holders of LNFA's ordinary shares in connection with the solicitation of proxies for the vote by LNFA's shareholders with respect to the proposed Business Combination and related matters as may be described in the Registration Statement, as well as the prospectus relating to the offer and sale of the securities to be issued in the Business Combination. After the Registration Statement is declared effective, LNFA will mail a definitive proxy statement/prospectus and other relevant documents to its shareholders. LNFA's shareholders and other interested persons are advised to read, when available, the preliminary proxy statement/prospectus, and amendments thereto, and definitive proxy statement/prospectus in connection with LNFA's solicitation of proxies for its shareholders' meeting to be held to approve the Business Combination and related matters, because the proxy statement/prospectus will contain important information about LNFA, ZeroFox and IDX and the proposed Business Combination.

The definitive proxy statement/prospectus will be mailed to shareholders of LNFA as of a record date to be established for voting on the proposed Business Combination and related matters. Shareholders may obtain copies of the proxy statement/prospectus, when available, without charge, at the SEC's website at sec.report or by directing a request to: L&F Acquisition Corp., 150 North Riverside Plaza, Suite 5200, Chicago, Illinois 60606.

No Offer or Solicitation
This communication is for informational purposes only, and is not intended to and shall not constitute an offer to sell or the solicitation of an offer to sell or the solicitation of an offer to buy or subscribe for any securities or a solicitation of any vote of approval, nor shall there be any sale, issuance or transfer of securities in any jurisdiction in which such offer, solicitation or sale would be unlawful prior to registration or qualification under the securities laws of any such jurisdiction. No offer of securities shall be made except by means of a prospectus meeting the requirements of Section 10 of the Securities Act of 1933, as amended, and otherwise in accordance with applicable law.

Participants in Solicitation
This communication is not a solicitation of a proxy from any investor or securityholder. However, LNFA, ZeroFox, IDX, JAR Sponsor, LLC and certain of their respective directors and executive officers may be deemed to be participants in the solicitation of proxies from LNFA's shareholders in connection with the Business Combination under the rules of the SEC. Information regarding LNFA directors and executive officers and such other persons may be found in the Registration Statement, including amendments thereto, and other reports which are filed with the SEC. These documents can be obtained free of charge from the sources indicated above.

About ZeroFox
ZeroFox, a leader in external cybersecurity, provides enterprises external threat intelligence and protection to disrupt threats to brands, people, assets and data across the public attack surface in one platform. With global coverage across the surface, deep and dark web and an artificial intelligence-based analysis engine, the ZeroFox Platform identifies and remediates targeted phishing attacks, credential compromise, data exfiltration, brand hijacking, executive and location threats and more. The patented ZeroFox Platform technology processes and protects millions of posts, messages and accounts daily across the social and digital landscape, spanning LinkedIn, Facebook, Slack, Instagram, Pastebin, YouTube, mobile app stores, domains, cloud-based email and more. ZeroFox and the ZeroFox logo are trademarks or registered trademarks of ZeroFox, Inc. and/or its affiliates in the U.S. and other countries. Third-party trademarks mentioned are the property of their respective owners. Visit www.zerofox.com for more information.

About IDX
IDX is a proven partner in digital privacy protection. Thousands of organizations and over 40 million individuals trust IDX to protect sensitive personal information from the growing threat of cybercrime. As a leading provider of data breach response services, IDX serves both public and private sector clients as an unparalleled strategic partner in data protection. Visit www.idx.us for more information.

About L&F Acquisition Corp.
L&F Acquisition Corp. is a blank check company formed for the purpose of entering into a combination with one or more businesses, with the intent to concentrate on identifying technology and services businesses in the Governance, Risk, Compliance and Legal ("GRCL") sector. L&F Acquisition Corp. is sponsored by JAR Sponsor, LLC, a newly organized special purpose vehicle under the common control of entities affiliated with Chairman Jeffrey C. Hammes, CEO Adam Gerchen, and Victory Park Capital. Visit www.lfacquisitioncorp.com for more information.