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 podcast interview first made available on May 2, 2022.

Welcome investors to The Absolute Return Podcast. Your source for stock market analysis, global macro musings and hedge fund investment strategies, your hosts, Julian Klymochko and Michael Kesslering aim to bring you the knowledge and analysis you need to become a more intelligent and wealthier investor. This episode is brought to you by Accelerate Financial Technologies. Accelerate because performance matters. Find out more at acceleratesshares.com.

Julian Klymochko: Hey, what's up everybody, welcome to the show. Today we are speaking cybersecurity with one of the leading experts, ZeroFox CEO James Foster. ZeroFox is an enterprise, software as a service leader, in external cybersecurity. On the show, Foster discusses what is so exciting about cybersecurity, the most important trends in cybersecurity that investors learn more about, details on the pending acquisition of IDX, a leading digital privacy protection and data-breach response services company, key factors driving the company's forecast 30% revenue growth rate and more, so please enjoy our discussion with ZeroFox CEO, James Foster. Welcome Foster to the podcast. How are you today?

James Foster: I'm good. How are you?

Julian Klymochko: I'm doing phenomenal, thank you. I wanted to kick things off by just going through your background, your career trajectory. Obviously, you've been focused on the cybersecurity industry for decades now, clearly an expert in the field. You've had stints at the U.S. Department of Defense, McAfee, other organizations. What gets you so excited about cybersecurity? What gets you up in the morning?

James Foster: Well, Julian, I think you just called me old. You told the world that I've been working on this for multiple decades. Look, I think I'm fortunate where I found a passion for cybersecurity in the late nineties, and I've just had the luxury of working in it my entire career. Now, certainly it was not the goal on day one. Wasn't even the goal at the halfway point, but it's an exciting industry. I think it's probably one of the only industries out there, especially in IT where I like to say that has multiple competitors. I'm always competing against my competition when it comes to go to market and keeping customers happy and just our place in the market. But you also have this entire other competitive set here, which is the attackers and the bad guys, trying to get past your software, trying to defeat it in every way possible. And so, I don't know of a world where I have that much competition that I get to get up in the morning, get excited about and energized and go after. And I've been doing it as you said for decades and that keeps me up and moving and motivated.

Julian Klymochko: So there seems to be guys coming at you from all angles. You got competitors on one side, bad guys, criminals, et cetera, on the other side. With all this competition in the market, what was the inspiration behind the founding of ZeroFox? And more importantly, tell us about the name. Where did the name come from?

James Foster: Look, we saw a gap in the market over eight years ago now when we founded the company in 2013, that was going to get created, we thought, because of social media, we said social media was going to change the world. And I'm not talking about the kind of social media that was being used for just personal connections, connecting with your friends, updating them on your status. We said that that fundamental technology would change the world because messaging would become asynchronous, and it would become on-platform. And so for the first, in the last 15 years, before the introduction of social media, people wanted to communicate via email and then chat came along. And in general, you could own the routing of that traffic, the routing of those communication messages, but social media represented on-platform collaboration. Nobody was able to even talk about collaboration prior to social. And we said: "We think there will be a world where every enterprise software platform wants to own the message, wants to own the eyeballs, wants to own the attention. And when that happens, it'll fundamentally change how enterprises acquire customers, go after employees and prospects, and how they engage with those individuals. And that new security would be needed to address that paradigm shift." And that's what we started building towards. And fortunate for us we were right, the world did adopt broadly speaking collaborative platforms. COVID certainly accelerated that the last couple of years and like most major IT industry adoption curves, security follows right behind it. You know, bad guys see that as a new opportunity, a new door, window into the organization and something they're aggressively exploiting and taking advantage of. And that's where ZeroFox helps customers today. We help identify everything that an organization has beyond their traditional firewall. Help them understand what it is and then help them protect those really important digital assets.

Julian Klymochko: You really nailed that call with respect to the growth of social media corporations wanting to own that message that goes through there, and ultimately that created that business opportunity in which you've founded ZeroFox. Could you give us the details on, you know, key elements of your business model? And in addition, I went through the investor materials, and noticed you have a forecast revenue compound annual growth rate, 30%. What's going to be the key drivers of this growth?

James Foster: Sure. Yeah. And I won't forget about the question on the name. I will come back to that as well.

Julian Klymochko: All right.

James Foster: We are an enterprise SaaS company, you know, the vast majority of our business is recurring in nature. You've seen that in the documents we filed with the SEC, but as a business model, I'd like to say we don't have a creative business model. And I think that's a plus, you know, we've adopted the enterprise subscription licensing agreement model. In general customers sign up for 12 months in advance, pay up front. And you know, they sign up for in general, one-year contracts. We do have customers that sign up for multi-year and that continues to grow year-over-year. And then some of the detailed financials that we have released, we've shown that we've been able to grow our large customer cohorts in a really nice fashion. I mean, we've grown six figure customers at a 50% CAGR or more in the last three years. And I think that really points to a few things. One, the maturation of this company. Our capabilities and our pace of innovation continue to demonstrate that we are able to help customers. And they're investing more in us as a platform to get broad protection. Two, is the maturation of the problem. I mean, this is one of those things where it's unfortunately the pillow I lay my head down on nighttime upon, when bad things happen in the world, it typically means good things for business and cybersecurity. And that's what's happening here in this space. There are more attacks every single week. And so, customers need broader and broader protection, and they need to be able to protect all of their assets, not just part of it. And so, we've been able to help them with that and grow into the platform we knew we could become. With the acquisition of IDX, it'll bring a really important strategic capability to our platform. We've been partners with them for over four years. We know these guys really well. They're an excellent cultural fit. They're passionate to keep the customers safe and secure like we are. They're passionate to push the pace of innovation and we saw an opportunity to take their breach response capability and identity protection capabilities, and put those on our platform, broaden our capability set and go after that larger TAM together. And because we had been integrated for so many years, because we had built trust and even go to market synergies, we just knew that this was a good opportunity for us. And as you saw, we're forecasting growth as a combined company. And we're an at scale company, we did north of $150 million combined last year.

Julian Klymochko: Now that acquisition of IDX is part of your recently announced going public transaction, which I did want to touch on. Prior to getting to that, one thing that I'm curious about is your company protects corporations from these bad guys. Have you seen any increases in activity? Increase in threats due to what's happening between Russia and Ukraine? Is there anything that's affecting your clients from that conflict?

James Foster: The simple answer is yes. And I'll give you some examples of why. I mean, there are things that are happening right now in the Ukraine - Russia war that are unique to this world. So one, the director of technology and digital transformation for the Ukrainian government went out on social media and open web almost four weeks ago now with a call to action for help, and blasted out via Twitter and Telegram saying: “I need help” and posted a list of things that they needed help with and think of that as cyber arms defense, it was basically a call to action to the world, anybody that was following and was a Ukrainian sympathist, I need help and here are discreet tasks in which we need help. That crowdsourcing of cyber defense has never really occurred at this scale before.

And having somebody that had an official post in a government saying, “We are being attacked and we need help,” asking for defense was a meaningful moment. And what happened at that juncture was there were thousands and thousands of individuals from the best that we could see that jumped in and helped out the Ukrainian government. And that was everything from defending assets that Ukraine had, to even targeting Russian owned assets, to try to disrupt some of their capability sets. And then at the same time, it created this situation where if you were a what I'd call friendly government to Ukraine, regardless of where you were in the world, and you wanted to now help with your cyber frontier or your cyber ops capabilities, you had a cover to do it because the Ukrainian governor asked the world. And so now, if you were an allied government and you had an intelligence or cyber capability, and you wanted to jump in, you could do it. And as we've seen, there was very little agreed upon playbook on how this works in the world today. And so, yeah, we've seen an increase in cyber warfare for sure. And it's happening across the world right now, taking place really in Ukraine and Eastern Europe and Russia. That's happened before, but not to the size and scale and what I'd call a level of sophistication that is happening right now. And where this has gone is we're seeing decentralized criminal groups as well, that are pro-Russia, looking for people that are attacking Russia companies that are sanctioning Russia, people that are moving out of Russia, move the businesses out. And they're listing those companies in these closed off forms and saying, these are new companies that are no longer doing business with Russia, let's attack them. And so, if you're against Russia and you made a public statement, your CEOs made a public statement, you've moved businesses out, you're taking part in sanctions, there is a heightened visibility and heightened risk profile for you as an organization. The exact opposite is also true. So, if you come out publicly as an organization and you're maybe pro-Russia and say: “Oh, you know, we're not taking out our businesses, we're not leaving. We're going to continue to do business in Russia. We're not going to close down our restaurants or manufacturing capabilities right this second.” Well, you're now on the opposite group, you're in a different forum with the pro Ukrainian sympathists, and you're being attacked there too. And so, what's really challenging here is, you're seeing agitators fight both sides, pro or against, and it's created a different situation where now your PR team, your marketing team, your CEO, your political alignment as an organization can become and create a greater risk for you or create a target. And those targets are cyber-attacks, they're hacks, they’re ransomware, they're digital boycotts of products and services, and things that are just really tough to consume and remediate. And so, it's created a lot of challenges where companies are reaching out and asking ZeroFox for help and saying: “What should we do? What's the strategy behind this? What kind of risk does this actually increase? And how should we think about this going forward?”

Julian Klymochko: And how does ZeroFox help those customers? Like what are some specific applications in which you can protect them?

James Foster: Yeah, sure. I mean, look, first of all a lot of the attacks that we're talking about right now are digital in nature, right?

Julian Klymochko: Yeah.

James Foster: When we talk about cyber war, they are by definition, digital attacks. ZeroFox is a leader in external cybersecurity, and this is squarely and solely what we work on. We work on external based attacks from external attackers. And so, the flip side of that coin is something that was really worrisome to the world. And the, you know, kind of roughly 2000 to 2010 timeframe, which is called insider threats. People were really worried about insiders plugging in USBs, taking away data.

Julian Klymochko: Right.

James Foster: Sending emails that had sensitive information to Gmail accounts, you know, leaving the building with source code, contact information, sensitive information. Now, what has everybody scared stiff is external attacks. People from nation states or cyber-criminal groups on the other side of the world that don't really fall under local jurisdiction or law enforcement capabilities. Constantly attacking them, putting ransomware on their computers that they have to pay big fees to get access to, and just becoming more than a nuisance. And so those types of attacks are how we help organizations. We help them understand what they look like to the exterior kind of part of the world, and then where they have vulnerabilities and assets that may not be protected. And then we protect them. So, we offer that end-to-end solution set to tell them what they've got and show them how to protect it.

[Word from Sponsor]

Michael Kesslering: And so, when you talk about that end-to-end solution and given the example of ransomware where there is an ask to get re-access to that computer, are you helping on that very back end in terms of, is there anything that you're able to help them with after the ransomware has been engaged on the system? What are you able to help with on that side?

James Foster: Yeah, that's a good question. So, look, if ransomware gets put on your system, you're in a response mode, first of all. And so, our goal is to make sure that never happens, right? And there are really good internal security vendors that are out there that are making sure that your devices are secure and your applications secure. CrowdStrike and SentinelOne, two new leaders that are out there for that internal security and device management. Like, they're great, think of that as next generation antivirus, but the problem is you can't just rely on that as your security stack alone, because at some point you have to realize when you rely on AV to do your protection of devices, you've already had multiple things failed. The attacks have gotten through, files have gotten through, and you've got to ask why that happened and where that happened.

And a lot of that happens in digital media as fake social media accounts can being created, connecting with your employees and sending them those files. It's fake domains, getting used to get those really annoying phishing emails that come through all the time. Five years ago, everybody was getting bombarded around wires: "Oh, can you send me a wire? This is your boss, it's really important. Call me on the weekend. Approve this wire", you know, they've changed some of those tactics to: "I need you to buy this Amazon gift card for me immediately and then call me later." And so those have now turned into ransomware tactics, which is same kind of urgency emails come through, but they leverage fake domains, and they leverage information that can be pulled out there. And so, in this world of digital media, if you buy or transact act online, I want to get to your customers, probably as much as I want to get to your employees because they're in the mode of buying.

And so all of those customers that live and thrive and have taken advantage of next generation media are the biggest targets. It's no longer just the banks. And I don't care as much about your employees and getting a $20,000 crypto payment. I care about defrauding your customers and stealing $150,000 in fraudulent customer orders before you know what's going on. And so, you know, part of your attack goals have also fundamentally changed and we help with that. And so, we help make sure that your again, digital persona and your external assets are identified and protected. And then in the unfortunate case that you have been attacked and you require breach response, that's a lot of where IDX comes in. They're the largest breach response provider in the United States. And they've been around for a long time. They were founded in 2003, they've got a great reputation, and we think that gives us a stronger value proposition to our customers. It's end-to-end, it is. I can help you proactively protect yourself. But if for some reason you know, an attack has occurred, and you need response capabilities up front and then put protection in after, that's fine too. We've got those capabilities as a firm.

Michael Kesslering: So, when you talk about, you know, some of this end-to-end protection, what sort of, from the customer's perspective, what are the economics of that? How much are they able to save by taking this preemptive approach as opposed to being more reactive?

James Foster: Yeah, the simple answer is more every year because the cost of a breach continues to increase. You've got dozens of states here, just in the United States, that have now regulation at the state level around what you need to do if you've got affected parties. And so, whether that's notification to compliance services that go in, that could be millions of dollars. And the U.S. is not alone here. Most of Europe, North America in general has regulation now that requires protection, notification and compliance related initiatives that have to happen when you've been breached. And what's going to happen here, the major movement that's happening across the world now is just recognition of when this has happened, because in general, two things have occurred and most chief information security officers, the CISOs, have gotten it right where they acknowledge what happened, they take accountability and ownership, they put a plan in place, and they just say: "Look, it's never going to be perfect security." And anybody that tells you, they have perfect security is foolish. It is, at best, great security that you'll have. And it's a game of risk management. How much resources do I have to apply to this problem set and challenge? And am I going to be as protective as I can, given the resources that I have? And because it will never reach perfect state, there's always going to be some residual risk that's out there. The CISOs that don't get it right, are the ones that don't take accountability. They try to stuff it under the rug when no one's looking, they don't provide notification. And it comes out a year later. It says: "Oh, well, yeah, we had that, but we didn't know the scope. We didn't do the real incident response. We didn't actually provide any notification. We thought it was just insider problem." And then it comes out to where it was much, much bigger than that. That's the wrong approach. And it's surprising to me still to this day, when you find out that organizations would rather push this behind the scenes, as opposed to own it, create a better posture, provide the things that they're required to do, and then just move on. And I think Wall Street's now rewarding those companies that take accountability and put robust plans of action in there, as opposed to the ones that try to hide it and cover it up.

Julian Klymochko: It seems like we're increasingly seeing these security beaches and incidents. So, I'm not surprised to see more and more corporations take a preemptive approach where they're looking for a company like ZeroFox to protect them, you know, risk management before it's too late, is what I say. Now with respect to implementing that protection for corporations, with your solution, understand that artificial intelligence, AI, plays a big role. Can you talk about how AI is utilized within your solutions?

James Foster: Sure. I mean, we've implemented multiple kinds of artificial intelligence throughout our platform. You have to to hit scale these days. I mean, data processing and the kind of data that we consume, our global data sets by nature, right? I mean, we can consume textual data, everything from dark web textual data that we get to open web data to social media that's textual that comes in. Where we receive and process high risk media content, whether that's pictures, emojis, videos, audio files, I mean, think of that as high risk media content and the types of processing that you want to do to look for attacks to look for things that could be nefarious is no longer just link analysis, right? I mean, the email guys had it really easy for 12 years where they just had to search for bad links.

Julian Klymochko: Yeah.

James Foster: And the malware guys sitting, you know, on your device had it easy, because they looked for files and they looked for known pieces of malware and viruses. And if that was the signature for a file, when they used to have signatures, they got it easy. Yes, this is bad. No, this is okay. And so, AI's been applied to this problem with us because the threats are constantly changing. And so, we've got things like computer vision capabilities, which allows us to deconstruct the picture and determine if there's an object in a picture. That's great when someone's trying to, you know, add your logo to a page for a phishing attack or maybe a fraudulent order. And so, me being able to identify if your logo's used inside a picture, it's not really possible without AI, right? And having computer vision capabilities there. We use things like neurolinguistics programming, NLP, to determine language sentiment you know: something mean, something happy or sad. We use the same thing for language identification: Is this Russia, you know, Russian, is this Spanish, is this English? And so, figuring out different kinds of language detection capabilities is also very useful. And then using those processing capabilities and combination is really where you get the strength of our platform, right? And so, being able to detect if something is a particular language, and if that is a place where you do business, determine if your logos also used is a part of that, determine if this is positive sentiment and an advertisement, and it's targeting somebody as well as it's got like a password button, because people don't want to type out the word password anymore, that's really easy to search for. Using those types of kind of building blocks together, gives you the capabilities of our platform to search through billions of things in real time and kind of separate signal from noise for our customers. It’s what we do.

[Word from Sponsor]

Michael Kesslering: And so, when you speak with investors, what would you say is the most important trend that they need to be following in cybersecurity to really thoroughly understand your company?

James Foster: Well, look, I think the security industry has had new categories get created over the last 20 years, but they've all been built upon the backs of new problems. And so, when I talked about this earlier, you know, security lags IT trends. When the IT boom happens, then ultimately the savvy and creative hackers of the world latch onto that to try to figure out how to exploit it, to kind of meet their objectives. And I don't think that's any different with security. And so, the real question I'd have for anybody is, like, do you believe that external attacks are going to go down or up? And if external attacks go down, if you find a way that you think that the government's going to step in and finally squash it at the governmental level around the world, or that our nation state adversaries that have sophisticated capabilities become friendly allies, you know, those are the kind of existential threats to this category if all of a sudden we were best friends with China or Russia, and that our nations weren't attacking each other on the cyber front, then that breed of attack would go away. We don't believe that's going to happen in the near future, unfortunately. And so, I think that's why we, as well as our investors are very excited about what we're working on and the ways we continue to help create successful outcomes for our customers. And I will say, as you mentioned, as we go public here, all of our investors are rolling into this. You know, this is a financing for us. It's not a liquidity event, we're not done. And so, I think they believe that we have a lot of work and a lot of opportunity in front of us. And I certainly do as well.

Julian Klymochko: Now I did want to touch on the recently announced going public transaction, merging with SPAC L&F Acquisition. In additionally, and this is fairly unique with respect to going public transaction. It does involve the acquisition of IDX, which is a leading digital privacy protection and data breach response services company. Also, as you mentioned, it represents a finance. So, a lot of things happening in this transaction. Can you talk to us, what you're looking to accomplish from this deal?

James Foster: Yeah, absolutely. I think the opportunity in front of us here and the catalyst was to merge with IDX. Like I said before, we've been partners with them for several years. We have mutual respect on both sides of the aisle. And I think given the technology integration we have, we approached each other last year and said, we think there's a really interesting opportunity to put the two organizations together for the betterment of our customers and create a broader platform to attack this market because the combination of protection and response just seems to swift fairly with what our customers really need today and what they'll need tomorrow. And we ended up financing that transaction with a SPAC. And so, I think the creativity that a SPAC can bring to the table in terms of leveraging public markets to finance two private companies coming together, we like that optionality that gave us, and we felt that given our size and scale and the number of customers we have in this really important market, that this was also the right time to be a public company.

We always saw the opportunity to be a long-term sustainable company. Because we thought the problem we're working on was really big. And it was never an artificial timeline of this is when we have to go public or else, we saw the opportunity and that's why we're doing what we're doing. And as you said, we have also got $170 million committed PIPE on top of the trust funds that are out there. And L&F has another $175 million in their trust today. And so yes, it should give us plenty of dry powder to continue to invest in innovation, grow organically and create other opportunities for us if we look at other strategic tuck-ins, that would be beneficial for the company as well.

Julian Klymochko: Thanks for that detail. That makes a lot of sense with respect to this merger. And if you do want to be active on the M&A front, then it certainly helps to have that publicly traded paper. Now, with respect to being a newly minted public company, as you mentioned, there's a lot of cybersecurity companies out there. What specifically, and what are the main factors that investors should know that would excite them about ZeroFox and your stock instead of some of the other competitors in cybersecurity?

James Foster: We will be the first company that's publicly traded working on external cybersecurity. That's the takeaway.

Julian Klymochko: Right, okay.

James Foster: And so, if you look at the other companies that are public, that are out there, they've been working on problems that have been around for quite some time. And a lot of those companies do a very good job at what they've always done a good job at. And so, you know, for example, there are three publicly traded security companies today that have high quality vulnerability management products: Qualys, Rapid7, and Tenable are three great examples of market leaders for vulnerability management. And they've changed the name, what that looks like over the years, but they've been around for quite some time. That's their space. And they look for, you know, they look for vulnerabilities in systems. As the first publicly traded external cybersecurity company, we have the ability to blaze the trail for our customers and look at the only company that's hit size and scale, that's planted that flag. And I think that gives them, you know, an extra confidence boost that I'm picking the right company. I'm picking somebody else that people are trusting, and they clearly have the capability to help us for several years. And I think that's really important in cybersecurity. Very rarely do customers, as I say, want to date their vendors in cybersecurity. They're looking for trusted advisors that know what they're doing. That'll be there for the long haul and it's not easy. This is not a, you know, sign up and put your software in and walk away. In cybersecurity, you need to be ready to pick up that phone on a Saturday evening, if there's something bad that's happened and respond within minutes. And that sets us apart and that customer commitment that's in our DNA, lets customers know that we're here for the long haul with them. And I think we put ourselves in a position to be a category leader for quite some time. And I think that'll be represented by continued scale.

Julian Klymochko: And the thing about cybersecurity and this day and age with so many threats coming at seemingly every business, if it's not something that you're worried about, it can be absolutely devastating for a company. So, it's certainly a much-needed service. And if investors are looking to learn more about ZeroFox and they're going public transaction, the ticker symbol of the SPAC L&F Acquisition is LNFA. And once you guys complete the deal, you'll be trading under the symbol ZFOX. So Foster, thanks so much for coming on the show today, sharing all the good stuff about ZeroFox and your story and the growth behind it. So, we wish you guys the best of luck.

James Foster: Mike, Julian, thanks a lot. It was a lot of fun.

Julian Klymochko: All right, take care. Bye everybody.

Thanks for tuning in to the Absolute Return Podcast. This episode was brought to you by Accelerate Financial Technologies. Accelerate, because performance matters. Find out more at AccelerateShares.com. The views expressed in this podcast are the personal views of the participants and do not reflect the views of Accelerate. No aspect of this podcast constitutes investment legal or tax advice. Opinions expressed in this podcast should not be viewed as a recommendation or solicitation of an offer to buy or sell any securities or investment strategies. The information and opinions in this podcast are based on current market conditions and may fluctuate and change in the future. No representation or warranty expressed or implied is made on behalf of Accelerate as to the accuracy or completeness of the information contained in this podcast. Accelerate does not accept any liability for any direct indirect or consequential loss or damage suffered by any person as a result relying on all or any part of this podcast and any liability is expressly disclaimed.

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 www.sec.gov 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 sector. L&F Acquisition Corp. is sponsored by JAR Sponsor, LLC, a 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.