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 from an investor presentation given during the Stifel Cross Sector Insight Conference held on June 7-9, 2022, and made available on the ZeroFox website on July 6, 2022.

Mark Baillie, Analyst, Stifel
Hi, everybody. I'm Mark Baillie, on the investment banking team here at Stifel. We are really pleased to present ZeroFox this morning as a participant and presenter in this conference and holding one on ones today. ZeroFox is a leader in external cybersecurity threat protection. Foster, the CEO; Tim Bender, the CFO are here. Tim will take the lead on the microphone on the presentation today. They are going public via the merger with a SPAC and are expected to be listed in trading within the course of the next six to eight weeks. We're excited to present them today. Brad Reback is the research analyst and obviously we'll be happy and available to take questions outside this presentation during the one on ones today.

With that, I'll turn it over to Tim Bender, CFO. Thanks.

Tim Bender, Chief Financial Officer
Thanks, Mark. Well, Mark stole probably my first four slides, so that'll help us move through the deck fairly quickly. Again, Foster and I here. We welcome the opportunity to tell you about our story and where we're going. So four pages of disclaimers, as Mark mentioned, we are in the process of becoming a public company through the SPAC transaction. So our information S-4 couple amendments to date, as well as this presentation and other information is on EDGAR under the ticker LNFA. So if you want to research any of our information, it's there, and of course read all the disclaimers and risks.

Mark mentioned quickly, we're going, we're becoming a public company through a de-SPAC transaction. So, first we're completing a three-way business combination where ZeroFox is merging with a company called IDX and then ultimately being acquired by L&F who is our SPAC sponsor. The transaction is being valued at a roughly 1.3 billion total enterprise value. We look at this as a milestone for ZeroFox. It's not a liquidity event. All of our shareholders are rolling 100% of their equity into the new ZeroFox, including Foster next to me, our CEO. So again, this is a milestone for us. We chose the SPAC route. We thought it gave us some unique capabilities and maybe an efficient process to complete our acquisition of IDX and become a public company.

And then I think the last and maybe one of the most important elements of this slide here is our deal is fully funded through our convertible note and common PIPE – our common equity PIPE, so $170 million proceeds into the company fully funded. So you've seen a lot of the SPACs lately struggle to get to that deal certainty. You know, we really are pleased with our SPAC sponsor L&F. I think we both share kind of that long-term vision for the secular growth that is external cybersecurity. And we'll explain that in a bit here. And again, just talking about our evolution to become a public company. We think we'll become the first publicly traded company that focuses solely on external cybersecurity. And we think that access to the capital markets will allow us to achieve what is our strategy and vision of becoming the category champion in external cybersecurity.

So what is external cybersecurity as we think about it? It’s the public attack surface that exists outside an entity’s firewall. So simply think about that as the open and surface web, deep and dark web, social media sites, collaboration platforms, code-sharing platforms, and mobile applications, all those make up what we call that public attack surface. How does ZeroFox address that? You know, we protect entities and we protect your digital assets by identifying and detecting the threats that affect your digital assets. And then when those threats turn into attacks, pre, post or during, we respond, remediate and disrupt those attacks. We think of external cybersecurity as a top three priority for CISOs.

And so if we want to look at this, we think the new modern tech stack for cybersecurity has three primary elements, and we’ll break them down simply: internal, edge and external. So in the internal you think, a lot of times you think of endpoint, so CrowdStrike, SentinelOne are kind of the leaders there, putting agents on devices, you also have vulnerability scanning and other elements of that internal apparatus. On the edge, you’ve got the firewalls or the perimeter proxy, what have you separating that traffic that is inside and outside. And so, you know, the names that you see there Check Point and Palo Alto with the next gen firewall, Fortinet and Zscaler with their cloud-based approach are the leaders in that category. And so that leads to external, right? And so, again, those are the assets, the operations that are happening outside of your visibility, your realm of control.

So think of a domain impersonation, information leakage on the deep and dark web things of that nature, your internal and your edge systems, aren’t going to find and identify those elements. That’s where ZeroFox comes in. Couple maybe real world use cases of some of the external protections that we provide. And this will show up a little bit later in our deck anyhow, but, let’s say your CEO, sitting here with Foster now, let’s say one of his social accounts is impersonated or even worse taken over. He might send – that account might send out information on the market, what have you, like an article from the Wall Street Journal or something, I look at him as a trusted resource.

I click on that. And next thing I know, malicious information has been downloaded again. He’s a trusted source, but that account has been taken over. Or maybe like domains, like if ZeroFox, if we change ZeroFox to putting a zero, instead of O into our domain, again, looks like a trusted site. A lot of times, I’ve got these glasses and I’m looking at my phone. If I don’t see it, I might click through something accidentally. And again, I then click on a link and next thing you know, malicious activity is downloaded and the adversary is off getting information. And I’ll give a real world example. I’ve got a vendor that I get their invoice via email. And in the header, it says our collection, our domain has been impersonated and our collections team are sending out invoices with incorrect bank accounts.

And then in capital letters, don’t click on that to make payment. Now, I wouldn’t do that anyhow, but, junior staff may because these go to multiple people. So there’s a perfect use case where I have a vendor that’s now in my pipeline. But that being said, there’s a perfect case where you’re seeing domain impersonation affecting customers. And again, that’s not getting picked up. Hence they would have to notify me that this is getting through their security apparatus.

And then maybe the last thing to talk about here is, like an incident of ransomware. Obviously ransomware very prevalent, you know, that has to breach all elements of your security apparatus to get through. Oftentimes, the external component, the part that we’re protecting those digital assets may be the most vulnerable or may not have the same level of protections that you’ve seen in the more mature markets like the internal and edge. And so again, that attack has a chance to build up outside of those systems and then eventually breach and get through. So as we think about cybersecurity, external cybersecurity and where we fit. We think that we are part of the three main elements and should be at the table with the CISO talking about these solutions.

We look at the market opportunity and we think it's big. We think it's growing and we think it's certainly maturing as we get there. And as we look at it here, we see it as a convergence of several different categories coming together. So if you look at it, vulnerability attack, surface, and digital risk, they play fairly seamlessly. You find assets out there that are outside of the firewall, you're able to provide protections. We did a couple acquisitions where we enhanced our threat intelligence capability. So now we're able to give our customers contextual data around the breach so they can understand the full scope. We're also able to take some of that data, that threat intelligence data that is either specific to the customer or just more in general and these customers can use it in their other security tools, to enhance their overall security apparatus.

And then as we'll talk a little bit about IDX, we'll be adding breach response as part of our capabilities and just feel that's an important market and an important element of the TAM that we'll be able to address. Regardless of how you size it, regardless of what specific piece of this puzzle you're looking at. If you look at Forrester and Gartner, they think it's an up and coming market and we certainly agree.

So what's happening, digital assets, the transformation is on, right? The way we communicate with customers, the way we communicate with employees, other constituents, it's all through digital channels now, right? So the digital transformation is happening and it's accelerating. We've obviously come out of a pandemic where we saw some of that even accelerate quicker than we thought prior to that. And so you look at what we call these crown jewels. If you look at these elements, and these are components of your workforce, your work apparatus. Now that is outside of your firewall. I'll give you an example, I see a lot of gray hair in here. So 15 years ago, right? We couldn't have social media accounts on our work devices, right? So now today, if I fast forward, you know, these tools have become important business tools.

Facebook from a marketing perspective, Twitter from a customer success perspective, LinkedIn that's the prevalent tool that my recruiters use is LinkedIn. Again, that's an application that sits outside a traditional firewall. And then something like digital currency, we're seeing nice traction there. These companies are built digital first, digital only from the ground up and that just gives them a large attack surface that's more ripe, right? So we see a lot of scams and frauds against the digital networks as well as the members in those networks. So what's happening is more and more assets are becoming digital. And that's just expanding the attack surface that an adversary has.

And because of that and because the adoption is increasing of all these different platforms, the adversaries take notice, right? They're going to go follow the trends of where they see business and activity and communications occurring. And if you look at that slide, we'll just quickly highlight somewhere between 8 and 10 years. If you look at the number of records exposed through breaches, a 40-fold increase. And so what's happening is because of digital transformations here, we're adopting these platforms and we're creating digital assets for use for business. It's expanding our attack surface, the risk profile for the company just gets elevated, which is where ZeroFox comes in.

And we aim to protect our customers with our AI powered platform. We have 20 patents today and many more in flight. So again, we're investing in our technology to solve our problems. So the first thing is, if we look to my left slide, you look at all the different platforms that we talked about. Many companies, many organizations don't know their digital footprint. So the first element is to help them identify it. You can't protect what you don't know exists or can't see. So that's the first element. So let's say you do that and you now start creating those, you identify those assets, those digital assets, and you want to go and protect it, look at the amount of traffic that's happening on these platforms. It's massive, right? And so ZeroFox has built a platform that has shown its ability to scale. We're analyzing this data. We're ingesting it, analyzing it, and then making, taking actions upon it.

And then the last thing I'll say about this slide, a lot of our competitors aim to solve the solutions or the problems for their customers, more at a point level, meaning like someone might have good domain protection where they're able to protect impersonating domains, but they don't have a deep and dark web capability. So they're not able to go out and find data leakage on the dark web or someone might have a decent dark web capability, but no other ancillary, threat intelligence or what have you. Social media is where we started and one of our strongest points as well. So we've taken the approach that this has to be a platform play to solve our customers' issues. And so that's why we've invested heavily in our platform. And if you look anywhere on the continuum NLP all the way up to the harder machine learning and computer vision, our customers are requiring a platform approach that addresses the whole ecosystem of external cybersecurity and that's what we're providing.

Real quickly here, our platform is able to provide continuous protection and continuous response for our customers. So if we look at this circle, we're able to identify and protect the digital assets. We have predictive capabilities. So we may see where the next attack is coming. If that attack is there, we have the ability to detect either pre or during the attack life cycle. And if it does happen, we have the ability to respond and disrupt those adversaries across the attack life cycle.

Which brings us to IDX. We looked at breach response as an important element of our external cybersecurity platform and our strategy. IDX is a leading breach response provider. Last year or over the last 12 months, they serviced over 1,200 customers experiencing a breach.

One contract IDX has is quite significant. So we'll talk a little bit about the U.S. Office of Personnel Management or OPM. Several years ago, OPM was subject to a nation state attack where several millions of records were breached and IDX won an initial contract, a multi-year contract, for $133 million. A few years later, they were able to upsell that. And again, a multi-year contract of $460 million that takes us through June of 2024. The program is funded through 2027, the contract through 2024. The contract generates $83 million of annual revenue for us today. It certainly gives us scale, gives us stability and gives us cash flow, meaningful cash flow to invest back into the business. And so, again, the size of this contract just shows IDX's ability again to handle the large-scale breach response and again several million members of ex-personnel and personnel of OPM are covered under this award.

With IDX into the fold, we believe now that we're able to provide our customers pre breach all the way through post breach capabilities into our platform. So if we look at kind of the color scheme on the red and to the left of the circle would be the ZeroFox capabilities. And we talk about, again, identification of your digital assets protection there, predictive threat intelligence through our threat intelligence teams. We're using artificial intelligence in our platform. You can see the number of breaches that happen. We're able to detect and prevent many of those early on in the attack life cycle.

During the breach cycle, we're able to add that response notification period and then should something happen, and we know they do happen based on the number of breaches, IDX is there to help with the ongoing breach response and monitoring.

Kind of talked about this slide. So everybody looks to put up their logo slide, right? And so, sitting through many of these presentations, everybody wants to show all their customers. And we certainly have a high list of reputable blue chip customer names. And I think for me, I want to talk a little bit, maybe pivot a little bit on this slide for those who are new to ZeroFox. And again, this deck is part of our public filing information. So we haven't updated some of the elements here, but real quick, a little bit to talk about our business model. We haven't chatted about that a little bit yet. So ZeroFox is a software-as-a-service business model, just like you'd see (everybody likes to use) Salesforce but we'll start with the Salesforce one down the line. Prepaid annual subscriptions are our primary contracting vehicle. And then we recognize revenue basically ratably over the term of that contract. So, pretty much you're looking at an annual subscription agreement. You could expect that revenue is going to be ratable across the board there.

IDX delivers their revenue through their platform. OPM we would consider as a recurring revenue source. And then the breach response is usually 12 to 15 month contract. And then once you are finished with that, the contract ends and that customer goes away. We did $150 million, roughly $151 million, of revenue on a combined basis last year, roughly 90% of that was recurring in nature. And again, we'll include OPM in that recurring number.

So one of the, again, talking about the numbers to the right on this slide. One of the numbers here that is encouraging to me in the six years I've been here, we show 128 of the Global 2000 that we have as customers. That's approximately 6%. So as we talk about the TAM, we talk about our runway for growth. There's tremendous opportunity to bring in new customers, new logo acquisition in that subset of cohort of customers.

We're going to do that through traditional field and inside sales. We segment our sales teams by customer size, but we have right now field and inside sales teams. Our centers of gravity are North America. We have London that covers primarily the U.K. and Western Europe and then the Middle East, we have coverage there. And then we've taken over the past couple years. We took a channel first kind of philosophy to sales. So we supplement our direct sales team with our channel network. And we're investing in building that channel network to bring additional growth opportunities for us.

Once you become a customer, you move over into our account management and customer success teams. Another lever of growth, and we'll talk about this in a few minutes here, is our ability to not only upsell, but cross sell our customers. And so, as the account management and customer success teams mature and grow and as we build out additional capabilities in our platform, we look to drive up that net retention number and we see that as a significant driver for future growth.

One of the things that we mentioned or when we talked about as we looked at our slides with IDX and ZeroFox, there's very little overlap in our customer base right now. So if you think about our ability to upsell and cross sell into those customers, right now, the IDX customer, we service the breach, breach is over. We move on, there's no opportunity, no other platform or capabilities for that customer to take on. So that's an opportunity for us, and we see that as a growth opportunity. And then, we're able to, if something happens to the ZeroFox customer base, able to provide that breach response capability.

So again, little overlap, and we see that again, as the ability to upsell and drive customer growth in that regard. And then the last number too, that again, is encouraging through my tenure with the company is we've seen enterprise customers or at least enterprise size customers, adopt our solutions at a nice clip. And over the past three years, we've seen the number of customers paying us over $100,000 and we look at that just as a metric that is important for us on our customer base as far as enterprise adoption. It's grown at a 50% clip rate annually over the past three years. So roughly 30 to 40 a few years ago, north of 130 now. And so again, we see those types of customers adopting our solutions, validating our market, right, validating our solutions, validating our approach.

Last piece with IDX, just we'll talk real quickly about their go-to-market. Talked a little bit about ZeroFox. A breach occurs and usually what happens is there's either law firms, professional service firms or insurance panels that run the breach response and the breach life cycle. We are, we sit on those panels. We have strong relationships with the firms that run these. And so when the calls come in, we're there, we're able to quickly respond. And because a breach has a certain sense of urgency, we're able to turn those responses quickly and win the contracts that we do.

Last piece with IDX and ZeroFox, we've known them for several years and through their services, we provide data services and other feeds to them to help power their services. So we knew them well, we've known them for several years. And that was part of the thesis of the acquisition. And we've already done some of the product integration that we need to do, because again, we're feeding their product from a powering source of giving the data protection to their customers.

I can't see the clocks. I don't know how much time I have.

Mark Baillie, Analyst, Stifel
Seven minutes.

Tim Bender, Chief Financial Officer
Seven minutes. Okay, perfect. So I want to talk about a couple customer case studies. Again, everybody has these slides, but again, to me, this is an example to talk about a little bit of our land and expand strategy and perspective strategies and just show how we can continue to take more share of wallet from customers. So the first is a large bank and several years ago, roughly when ZeroFox was first started, they had an issue with executive impersonations on some of their social accounts. So that was ZeroFox's basically strongest component seven, eight years ago. We started out with a contract for roughly $300,000 providing executive protection across social accounts.

Over the past several years, we've added a multitude of services for domain and brand protection. We're providing threat intelligence. We're providing threat feeds that get used in other elements of, again, their security apparatus. So our intelligence and data is being used to fuel to help strengthen their security profile. We've added disruption across all elements of their business. So we've taken a $300,000 customer and taken it to over $2 million in annual revenue and they've signed up for multi-year deals.

The second is an example of IDX. Basically a large automotive manufacturer was breached maybe six, seven months ago, I think that was about the timeframe. Several million, as you can see, cases or records of data were compromised of their customers. IDX was able to quickly respond, again, to the reach out by the firms running the breach and in doing so won an award that's going to generate more than seven figures or $1 million in revenue.

So again, IDX not just in the OPM realm, but IDX is able to show their scale of solutions to a large set of customers that are affected by breaches. One of the other elements I think that, again, is encouraging for us as we look at moving this forward. We know when customers get breached, or we know when customers have an incident, they call us. They're likely to buy something from us and they're likely to buy in a compressed sales cycle, right? Because obviously they're having an issue. So in this case, this customer has an issue. As a combined company, we have the ability, once we get past looking at the first initial kind of breach response set up and going forward, we now have the ability to have that dialogue with a CISO to add, protective services on the front of the – if we go back to the circle to the left side – the prevention side of their protective services.

So again, more capabilities to sell to customers. And then the last just a small breach at a government institution and not big, nowhere near the size of the one to the left. IDX responded, has breach response care for that. But then what happened is that entity, that organization said, hey, we need to take a bigger look at our security profile. Like, what are we missing and in doing so, again, because of our relationship with IDX, we were able to come in and sell them that prevention and detective capabilities that ZeroFox offers as part of our external cybersecurity solution. So again, the upsell value on this one, you know, put there for effect, it's pretty high. Not every customer will have that upsell capability. But what we want to show is, you have an incident, it means you're going to start looking at other elements of your business, and that's where we can come in and add that upsell and cross sell capabilities.

So we'll leave with this. We think ZeroFox and external cybersecurity is a compelling investment opportunity and seven bullets on here, but really there's kind of three takeaways. The first is, this is a market that we think is growing, it's large already. And I think it's only going to continue to grow as we see the secular trends and digital transformation continuing. So as we showed earlier, kind of in our customer cohorts, there's a lot of runway for us. There's a lot of market out there for us to go get.

I think the second thing is, what we've accomplished to date is we have a high quality, high reputable customer base. So we've already seen enterprise quality customers adopting our solution, and we've built a platform that can address those needs, right? We're not building one element of the external cybersecurity ecosystem. We're building a platform that can address everything. So if you need curated threat intelligence to complement digital risk and other elements of your security, we have that. If you need domain protection, we do that. We disrupt better than anybody else and that's where we play.

So again, our platform is designed to meet the enterprise needs of customers. And then the last is our management team. We've been together, most of us for, you know, six plus years. Myself through SaaS business models for 20 years and Foster and our other senior executives with multiple years of cybersecurity. We are focused on the opportunity ahead of us. We want to execute that strategy that I mentioned before, where we want to be the category champion in external cybersecurity. And that's what we're set out to do. So that's it. Thanks guys.

Mark Baillie, Analyst, Stifel
Perfect. Thanks so much.

Q&A

Mark Baillie: Have any questions? You got a question.

Question (Audience): Just one question, given your success in the enterprise space, just curious as to your thoughts in the personal cybersecurity space. Do you see an extension for your technology moving into more down the road an opportunity, or is it something that you're purely focused on enterprise?

Answer (James C. Foster): Well, I'll take this one. I think we have plenty of opportunity to continue to focus our efforts on enterprise. There is a reasonable amount of our business that is inbound. If you think about the commercial markets that are out there that continue to get hit at a rapid pace. Tim talked about a 40x increase in breaches and attacks that have been experienced for the last handful of years. In general, when there's a problem like that, they go looking for the leader. Your house is on fire. You don't go looking for the best value at that point. The negotiation process is pretty quick. And all of what Tim talked about is absolutely true. We've got 6% of the kind of Global 2000 today. I could double that and double it again over the next few years and not take my eye off that ball.

My ASP is already larger than many of my cohort peers that are publicly traded today. My ASP was larger than Mimecast before they got privatized, it's larger than Rapid7 who's performed really well in the markets. If you look at some of the other guys that are out there, that shows you that I've got a real capability to solve enterprise quality problems. But the other corollary there, when you look at ASP tracking for enterprise organizations on a platform, is the size of the problem you're addressing for customers.

The security industry can be pinpointed by size of problem and longevity of problem. You've seen security companies fizzle out because the problem went away. Microsoft solved it with their operating system fix. Maybe they found an easier path of exploitation. We don't have a single, what I call existential threat like a Microsoft or Apple changing something and saying, oh, well, we'll fix this on our own. So I think there's really an interesting opportunity for us to continue to focus on our ASP and our enterprise base. That doesn't mean we're going to take our eyes off other opportunities in future as well though.

Mark Baillie, Analyst, Stifel
I think we're out. Thanks for the question. Any other questions? I think we're done. Yeah.

James C. Foster, Chief Executive Officer
Thanks, everybody. Yes. We'll be around all day.

***

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 Securities and Exchange Commission ("*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 (the "*Registration Statement*"), 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 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 certain securities to be issued in connection with 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 May 27, 2022, the record date previously 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.