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 Jefferies Software Conference held on June 1-2, 2022, and made available on the ZeroFox website on July 6, 2022.

Analyst, Jefferies, LLC
It's my pleasure to introduce ZeroFox. The leader in external threat detection and with us today from the company is Tim Bender, the Chief Financial Officer. He's going to walk through the company and we're going to have some time for Q&A at the end. So without further ado, Tim?

Tim Bender, Chief Financial Officer
Thanks, John. First, I'm really excited to be here this morning to tell you guys about the ZeroFox story. And then what I think is a compelling investment opportunity for a category leader in external cybersecurity. Couple quick housekeeping points. We filed our first S-4 maybe a couple months ago. We filed a couple amendments since, so our information is public. This presentation is available now in EDGAR. So read the disclaimers and risk factors that are contained therein.

Okay. So let's first talk about the transaction, what we're trying to do here. We're completing a three way business combination where ZeroFox and IDX are merging, and then we're merging with L&F Acquisition Corp. We chose the SPAC route because we thought in our environment, last summer, that this was the most efficient process for us to complete the acquisition of IDX and then for us to become a public company.

The transaction is being valued at approximately $1.3 billion in total enterprise value. And from the ZeroFox side, we're looking at this as a milestone and not a liquidity event. All of our shareholders are rolling 100% of their equity into the new ZeroFox. And if my CEO and co-founder were here today, Foster, he would reiterate, too, that he's rolling all of his equity into the new company. So again, milestone, not a liquidity event. And then finally, I think this is really important. Unlike a lot of transactions that are happening out there now in the SPAC world, our transaction is fully funded. We have a $150 million convertible note and a $20 million common equity PIPE that fully funds our transaction and limits our deal risk.

We're really fortunate to have L&F as the SPAC sponsor and our partner in this endeavor. And we're fully aligned with the secular trends around external cybersecurity and the potential for us to create long-term shareholder value for our current and prospective investors. So what is external cybersecurity and who is ZeroFox. Simply put, external cybersecurity is the public attack surface that exists outside your firewall. So think of that as the open and surface web, the deep and dark web, social media sites, collaboration platforms, code-sharing platforms and mobile applications. ZeroFox protects, identifies, detects those threats, and then responds to the threats that exist in those platforms that affect a company's digital assets.

We view external cybersecurity as a top three priority for CISOs today. When we think about the modern tech security stack, we think of it in three elements: internal, edge, and external. Internal, those are companies like McAfee and Symantec that have owned this market for roughly 20 years. And now you look at CrowdStrike and SentinelOne as the category leaders. What does internal do? It seeks to protect devices by installing agents, right, to protect endpoints and they could be delivered via the cloud or on-prem.

And then you have the edge or the perimeter, the proxy firewall. These guys are basically separating traffic from outside and inside, right? Whether it's logical or physical means appliances or cloud traffic that's being routed through proxies. You think of companies like Check Point, you think of companies like Palo Alto with its next-gen firewall, Fortinet, and then Zscaler with its cloud-native approach, which brings us to external, right?

And again, that's everything that the internal and the edge systems can't protect, and those are the things that they can't see outside of an organization's control or visibility. And so, again, we talk about a domain that might sit outside a company's purview and what do we mean by that? So let's take a domain like ZeroFox and someone replaces one of the "O"s with a zero. It looks like a legitimate website, right. But then people start accessing that site and then clicking on links or downloading information. And now a malicious payload is delivered. Or we think of one of our longstanding prominent use cases, executive impersonation. So the digital persona of a Fortune 500 CEO is compromised. And maybe he or she has her Facebook, LinkedIn account, and it might be compromised or even taken over.

And so that looks like a trusted resource. So when that person communicates with employees, partners, customers, what have you, people think of it a trusted resource, they go to that person's link, post communication. And again, malicious activity can be transmitted in that matter.

So the last piece that maybe we'll talk about, little bit about, this new modern tech stack is maybe a ransomware attack. And so if you think about a successful ransomware attack, that basically has penetrated all three levels of your security stack to get through and be successful, right? So we think about the edge guys aren't providing endpoint solutions. The guys in the internal aren't certainly proxying traffic and ZeroFox is dealing with neither of those two, right? We're focusing on external.

So if you think about an attack that might start in the external realm, first of all, that's probably the most vulnerable. A lot of assets are out there that people may not know about that filters its way all the way through and gets past your endpoint. Next thing you know, you have a ransomware attack. We like to think of your endpoint as your final layer of defense and not your first layer of defense. And some companies maybe think they have endpoint covered and that's all they need in today's world. So we look at internal, edge and external as kind of the trifecta of the new security tech stack and why we think ZeroFox is a leader in that category is part of the conversation.

Listen, I think the market is ahead of us, the opportunities there. This market's growing, right? And so the way we have viewed this market is as a convergence of several different markets coming together. So if we think about vulnerability and attack surface management and digital risk, those seamlessly play together our threat intelligence capabilities. Allow us to provide contextual data around breaches and attacks that customers can use, not only to better our platform, but can also put that information into their other security tools to help their overall security profile.

And then as part of this transaction, we're adding that breach response people. So once an incident does occur, we can take care of customers all the way through the full breach cycle.

So the age of digital transformation. It's accelerating, it's happening. That secular trend is affecting external cybersecurity. So again, we think about how companies communicate with each other, it's through these digital channels, right? So if we look at what we call these crown jewels. Personal example - social media. 15 years ago, we weren't allowed to have social media sites on your work devices. Now, take my recruiters for example, they can't recruit without LinkedIn. And so whether it's Twitter for customer satisfaction, whether it's Facebook for marketing, these tools that were once more consumer-oriented applications have become integral business applications. And they're not going to go through the same security channels that some of your other vendors and other suppliers will. Another example is, the digital currency, like these companies have been built from the ground up from a digital-first, digital-only approach. And so the number of digital assets are there, they're out there and they're more ripe for attack. And then their customers are getting hit with scams and frauds on these digital platforms. So basically, what's happening is the proliferation of digital assets is growing, which is increasing an organization's attack surface.

And as that attack surface is growing and as companies are adopting more and more of these platforms business, the attackers have seen it, right? And so if you look at this slide here over the past six or seven years, you see the number of records that have been exposed via data breaches has grown nearly 40-fold, right? And so, what's happening is the risk to a company is just growing and growing as the amount of digital assets and records are being exposed to the public, which is where ZeroFox can come in. So with our AI-powered platform, we're able to provide the protection needs that customers need as far as addressing the external cybersecurity issues. Today we have roughly 20 patents issued with more in flight. We continue to invest in things like computer vision, machine learning, natural language processing, et cetera, to enhance our platform. And we continue to make investments in R&D.

So if we take a look at some of the logos on the left hand slide, a lot of companies don't even know their digital footprint, right? So we walk into an office and are like, what do you have? They're not even aware of what they have. So if you look at the number of different platforms that exist out there, you can't protect if you don't know something exists, right? So the first thing is identifying what exists. Once you've done that, now you look at the massive amounts of data that you've got to protect, the sheer size of the amount of communication that's happening on these platforms is massive.

And ZeroFox is able to scale, our platform scales. We handle all this data. We collect it, we analyze it on our customer's behalf. The sheer size is overwhelming. And you need a solution that can handle that. And that's what we've taken the approach. We've taken the approach that a platform solution has to be the approach in this case. So that's why we've invested heavily in R&D to build a comprehensive platform to address our customer's needs.

Our platform allows us to provide continuous protection and continuous response for our customers. So we start – we're able to protect assets that exist, we're able to predict what might happen next when an attack is happening, we're able to detect it, respond to it. And then ultimately, kind of disrupt that. And in doing so, we're able to take a company's risk profile and bring that down through the use of our platform. One element of external cybersecurity that we think is important is the breach response piece. And we feel like that allows us to add the full breach cycle for our customers, as far as the external cybersecurity market. And in this case is a strategic driver, why we went ahead and decided to acquire IDX.

So IDX is one of the largest breach response providers around. They roughly serviced 1,200 customers last year. So 1,200 breaches, they were providing breach monitoring care to. One of their customers is quite significant. It's the U.S. Office of Personnel Management, OPM. OPM several years ago was part of the nation-state hack where millions of personnel's records were exposed. IDX won that contract initially at $133 million back in 2015, subsequently was able to expand that contract to over $400 million. And right now, today that contract generates about $83 million in annual recurring revenue.

And so that predictability and stability is important for the company. And then the cash flow that this contract generates is really important too, kind of our long-term vision.

So we think with IDX and the breach response, we're able to provide customers, again, that full life cycle care of pre-breach and post-breach. So, as we talk about the different elements of this ecosystem, ZeroFox would be obviously on the pre-breach side through our protection and detection identification capabilities. And then from there we have predictive intelligence, and then we're able to deal with the life cycle of a breach through response and disruption. If something does happen to a company and you certainly see by the number of breaches that are occurring, something will happen at some point. IDX is able to come in and give that post-breach care and that monitoring through the life cycle of that contract with that customer.

For those who don't know much about ZeroFox, I'm just going to quasi pivot a little bit here and talk a little bit about how the go-to-market of these companies – it's a little bit different – but how we come together, and give maybe a little bit of background on ZeroFox and IDX as a combined business.

First of all, ZeroFox has what I would consider a fairly traditional go-to-market engine. We have field sales and inside sales that are focused on new customer and new logo acquisition. Several years ago we made the decision to be a channel first company. And so, we built out our network of channel partners that complement our field and inside sales teams. We support those sales teams through your traditional digital marketing, ABM for our high value accounts and then field marketing events. So, if anybody's here next week down the street we will have RSA. We see field conferences and in-person conferences are coming back online.

Once you have become a customer, we turn you over to our account management and customer success teams who are responsible for obviously the account renewal and upsell opportunities. On the IDX side, most of their business comes in, what we considered a channel, but it's a little bit different. It's kind of a referral approach where you have professional or law firms, or you have insurance panels that usually run the breach process. And we have strong relationships with those parties. And when the call comes in, we're able to quickly respond and are able to submit proposals to win the breach contracts.

From a business standpoint, ZeroFox is fully a SaaS business model with prepaid annual subscriptions. So, just kind of down the straight narrow and what you see in most SaaS models. Roughly 90% of our revenue is recurring in nature. We're including OPM in that. The 10% that is not is this post-breach monitoring. These monitoring contracts usually last 12 to 15 months and then the customer no longer has to provide that monitoring to its members or its employees.

That's also opportunistic for us because right now IDX doesn't have that ability to extend that relationship. We have that ability to extend that relationship through, again, the protective services, the proactive services that we provide. What we've seen in our company on the ZeroFox side is if someone has an incident and they give us a call, they're likely to buy our services and they're likely to do it in a much quicker manner, as far as the sales cycle, as opposed to just going through, the cold calling or digital marketing approach.

So when someone has an incident, they're usually going to come and buy our services in a much quicker manner. Well, these IDX customers obviously have an incident, right? So we look at that as a right set of customers for us to go out and cross sell and upsell our broader capabilities. So we, again see the ability to cross sell and upsell to the different customer bases based on the needs that those customers have in their life cycle.

One other point real quickly too, is we have been providing and powering certain IDX of their product solution right now. So we know the company well. We've been a partner with them for several years and some of our product sets are already integrated. So we look at that as a company that we know well and we can take advantage of that.

We talked about this already.

Everybody has slides with logos, we have high quality customer slides.

I want to point to the – some of the data on the right hand side, again, that I think is really encouraging for us. Several of the Fortune 10, but only 6% of the Global 2000, so as I look at our ability to grow and acquire new customers certainly at the enterprise level, there's a lot of runway ahead of us, and there's a lot of opportunity ahead of us. And then the last slide or last number here, that's encouraging to me, being with the company for six plus years. The trend we're seeing in customers that are paying us more than $100,000 annually in contract value or revenue, we've seen that grow over the past three years at a 50% clip. And so we see that as, again, the continuing adoption by the enterprise quality customers for our solutions.

A couple quick customer case studies. And I think this is a good example of how again, in our model, we're able to attract new logos, but then also show some of the upsell capability. One is a large bank that started with us way back in the beginning, executive impersonations for some of their executives was their first use case. Over time, we've been able to add domain protection and brand protection. We started adding threat intelligence, so curated threat intelligence that allows our platform to perform better, but also for them to integrate into their other security tools to bolster their security apparatus.

And over the course of roughly seven to eight years, we've taken that customer from roughly $300,000 to over $2 million annually.

The second is an IDX example where fairly recently, a large automotive car manufacturer had millions of records exposed and were subjected to a breach. IDX was able to respond again to that inbound. Won the contract, the result is a seven figure $1 million plus basically annual contract to provide that breach care.

And the last one is an interesting example where before the companies actually came together. We had a part, the U.S. government had a small part that was subjected to a breach and not necessarily a large breach, but subject to a breach where then IDX started providing individual protections for some of the members in that organization. Well, that forced the organization to take a holistic look at their security profile and in doing so, identified a gap where they said, hey, we could use executive protection and we could use other protections like brand and location protections. So, not just some of the physical assets, but being able to protect some of the digital assets. And so the upsell value here is 50x, not necessarily what you see in most upsell opportunities, but the idea is something happens and forces the company to look at their whole profile. And that's where we feel like we can come in and take advantage.

I want to conclude with why we are encouraged and why we think this is a strong investment opportunity. A handful of bullets like everybody has. But I think the three big takeaways that I have from this slide is, one, there's a large market, it's growing. And we think as a category leader that we're going to be well positioned to take that market. We're seeing the secular trends with digital transformation contributing to the growth in this market. And so, we feel like we're in a great spot. And again, this transaction allows us to capitalize on that opportunity.

The second thing is, between bullet points two and three, we built a platform that's robust. Again, we built it – we solve the problems of our customers through the technology we built, as evidenced by the patents, by the evidence of the AI underlying our technology. But we also have customers that validated. ZeroFox has roughly 800 customers and those customers are validating the need for our solutions in the market that we're serving.

And then I think the last thing that I'd like to just bring is, our management team has numerous years, most of our executives are 15, 20 years plus in cybersecurity alone. And then, working for a SaaS business, myself, specifically a lot of us have experience in the SaaS industry. So our management team is committed to executing on our vision and strategy to become that category champion in external cybersecurity. Thanks for your time today.

Analyst, Jefferies, LLC
We have time for a couple questions, if anybody has.

Q&A

Question: Can you talk a little bit about how you're experiencing the labor markets these days and demand for cybersecurity personnel? How that's impacting profitability? Thanks.

Answer (Tim Bender): Yeah. So if I heard the question was how we're dealing with labor. I think we're not different from a lot of companies that are experiencing high demand and increasing salaries, labor especially in our engineering, but we're also seeing it in our sales and marketing. So we combat that in a couple ways. First of all, I think from a labor standpoint most of our engineering now is or most of our new hires are happening in Santiago, Chile. That's our center of gravity for engineering. It's in the same time zone, roughly as we are, we're a D.C. Baltimore based Mid-Atlantic type company.

So that's one way that we've been able to combat some of the labor challenges we see as far as compensation. From a sales standpoint, again, it's being just competitive with compensation that reflects where the market's going. But certainly like most companies, labor demand is there. From a security operations standpoint, we have a center in Bangalore, India where we're able to do some of our security operations at lower price points. So that helps us there.

Analyst, Jefferies, LLC
With that, Tim, thank you.

Tim Bender, Chief Financial Officer
Thanks, again.

***

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.