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 June 16, 2022.

James Foster, CEO at ZeroFOX — Heading Off Hackers: Why external cybersecurity is not just a defensive sport

Tom Ryan (00:00):
Hey, there. It's Tom Ryan, founder and CEO of ICR. Before we get into the next episode, I wanted to ask that you subscribe to the show. It'll help us get even more unique and interesting guests on the podcast. And in turn, continue to educate management teams and the growing ecosystem that creates value for fast growing private and public companies. And while you're at it, head over to Apple podcast and leave us a five-star rating, very much appreciated.

James C. Foster (00:29):
Security doesn't sleep. You have to be up and operational 24 hours a day, seven days a week. And your customers expect that you're constantly watching their back, especially on nights and weekends.
We've been global, operating around the clock for quite some time now, in general because attacks don't stop either. Our customers are getting attacked seven days a week around the clock.

Tom Ryan (01:21):
Being a public company can be hard. Small missteps can have outsized consequences. I'm Tom Ryan, founder and CEO of ICR. And over the last 20 years, we've helped thousands of companies understand and navigate the stock market and the media. We'll demystify these and other increasingly complex stakeholder groups so you can focus on what you do best, building your company and unlocking your true potential. This is Welcome to the Arena.

James C. Foster (03:24):
External cyber security is everything beyond your traditional firewall. Internal cybersecurity has been around for decades. I started my career off in the internal side of the house. That's really technology and the services protecting devices. There are great companies out there that do that, next generation endpoint security companies doing that. CrowdStrike and SentinelOne both come to mind for great internal cyber security companies, and they make sure your laptops, your servers, your mobile devices, they're all locked down, protected and safe.

There's another category of cybersecurity companies called perimeter security or edge security companies. These guys are firewalls, whether they're next generation firewalls in the cloud or actual appliances that you're installing around networks and office spaces around the world, these organizations separate the inside from the outside, and they're important. They try to keep the bad out.

ZeroFox focuses on everything beyond that traditional firewall, where we're looking for the things that could be targeting or damaging your business beyond the firewall off of your devices, off of your network, and making sure that you know what they are, and we can help you focus on eradicating those risks to the business.

Tom Ryan (04:29):
Yeah. Maybe give the audience a little sense of like the scale of the business, because I was really surprised at how big you are already and what kind of global reach you have.

James C. Foster (04:41):
We've been at this for quite some time now. I like to say we are a startup that's been around for about a decade and we're looking forward to going public as a milestone. It's not an exit for us. This is just another milestone on our journey. You know, we've got thousands of customers in over 50 countries already. We've got over 700 employees in the combined organization. I mean, we are certainly at a scale that's relatively unique in the cybersecurity space.

The great story I heard recently was there's roughly 1,600 cybersecurity companies around the world today. And I think about those cybersecurity individuals standing on a beach, looking at the surfers and the waves. There's less than two dozen people in the public markets and cybersecurity surfing those waves. So we are looking forward to joining those surfers on the waves, riding this turbulent market that we're in right now, and achieving another significant milestone on our journey here to really protect every company regardless of size or location around the world. They're all facing external cybersecurity threats.

Ransomware is the real notable attack that everybody keeps talking about, but a ransomware attack by definition is somebody outside your organization has targeted your organization, has found a way in, compromised it and is now holding you up for ransom. Those are the types of things that keep CISOs up these days. And those are the types of things that we help organizations with.

Tom Ryan (06:02):
It just seems like a constant never ending barrage. And as I hear you talking, there's certainly like a massive secular trend behind the business. As every business shifts to digital, it just seems like they're more and more vulnerable. Is that a good way to think about kind of the market for what you do?

James C. Foster (06:20):
It is. COVID was really an accelerant for us. Everybody left their office. Everybody left the comfort of the network security that was put in place over the last 20 years. They left their secure office buildings that had perimeters and appliances and these devices and desktops that were hardened down at your office for the last 20 years and said, "Okay, now you've got to work remotely."

And so the entire world accelerated their digital transformation plans. Everybody was working remotely. Everybody was hybrid. This adoption will be around for a long time. I don't think it'll go back anytime soon to where everybody's in office. And it's created this entire expanded public attack surface because companies have really adopted 10 years of digital technology in just the last two or three years. And it's left them incredibly vulnerable.

We've seen the number of breaches go through the roof and the number of attacks on organizations go through the roof because they've got all these new investments that they had to jam in really quickly and security in general was an afterthought. You know, productivity was the goal out of the gate. And we've seen that time and time again over the security industry in the last two decades and companies are really paying for it now, unfortunately.

Tom Ryan (07:31):
It seems like the market for external cybersecurity is not as mature as that internal model, which is kind of what you're talking about. What is the market opportunity for external cybersecurity, which is where you guys shine?

James C. Foster (07:45):
Tom, that's exactly right. It is less mature than internal. I mean, the oldest markets in cybersecurity in general, there's a few of them is device security. Old school antivirus has been around a long time, more than a couple of decades. Firewalls have been around a long time, more than a couple of decades. And, really, the external cybersecurity market that we live and breathe in right now is relatively new to the game.

These digital platforms that every business is thriving on these days, that's allowing us to collaborate with our employees, collaborate with our customers and prospects, identify leads, sell services and products, they're relatively new. And on-platform collaboration is relatively new. I mean, shoot, if you go back even five years, the word collaboration didn't mean what it did today. Slack and Box and Dropbox really kind of drove that collaboration mindset and enterprise organizations.

And that collaboration really changed the entire industry to where owning communication, owning the eyeballs of a consumer and keeping them on your platform is the most important thing. And so before, security teams really needed to lock down the web and lock down email, but now they need to make sure they understand every single platforms their employees are active on and the security risks that get brought into those organizations because of that.

And it's leaving a lot of doors open and a lot of windows open to their environment. And that's one of the reasons that you've seen breaches just go through the roof.

Tom Ryan (09:21):
What is the breach rate for companies or the industry today like versus five years ago, and then 10 years ago? It must be exploding.

James C. Foster (09:29):
It is exploding. We published a report earlier this year at ZeroFox that said over 50% of the companies that were out there got attacked and some sort of compromised last year. I mean, that's just staggering. And so it's no longer a question of, will you be attacked or will that be successful? It's really just a time of when and what will the impact be?

And what we've seen here is an additional shift in regulation where the SEC is adopting new rules around notification of breaches, the timing that's required and the level of notification. And so for the first time ever, companies that are now getting targeted and breached, public companies, they're going to have to report that and they're going to have to report it really quickly with some accuracy. And I think the market will take notice if you make a mistake on those notifications.

So if you don't have the right capabilities to understand the scope of the breach quickly, what you're going to have to do is then subsequently disclose that your initial notification to the SEC was wrong and it was bigger than you thought. And the only thing worse than having a breach is having a breach that's bigger than you thought then having to retell the world over and over again. "Sorry, it's even bigger. Sorry. It's even bigger."

Tom Ryan (10:45):
I'm cringing just hearing about it, imagine being a CEO and having to talk about that. It's painful enough to handle it communications-wise, let alone the logistics and execution of handling a breach. One thing I wanted to ask you, Foster, is being in 50 countries while there are a lot of companies that focus on cyber security, you're doing it at scale. How does that help the average customer that you have?

James C. Foster (11:09):
It's been a competitive advantage of ours for quite some time. We took a global outlook on the business, our customer opportunity, and then also the problem set that we're addressing. We've got employees around the world. We've got major security operations centers in multiple countries around the world. Running a 24/7 shop is something that our customers have come to expect. It's not a nice to have. It's a must have. You have to be up and operational 24 hours a day, seven days a week. Security doesn't sleep. And your customers expect that you're constantly watching their back, especially on nights and weekends.

And so we've been global operating around the clock for quite some time now, in general because attacks don't stop either. And so we've got the stats to back up that our customers are getting attacked seven days a week around the clock. Where I think this gives us a competitive advantage is the fact that we are embracing our global strength and size and scale.

And so, you know, being able to serve your customers in region, in theater, understanding cultural intricacies and nuances, given that you've got a global employee base is very important. I think a lot of American tech companies think that they've got tech that scales because they've got the AWS bills to prove it. And they missed the small nuances of working with customers and the way they want to be treated and worked with. And something that we are very prideful of is that we can help our customers in region and theater around the world.

It's not cheap to get global either. We've spent tremendous amount of money investing in our global workforce.

Tom Ryan (12:47):
It makes total sense. Shifting gears a little bit, tell me about the go public transaction with L&F and what that does for you. I know you referenced it as part of the journey. I always say that most people around a company going public, all the advisors, it's kind of like the finish line for them. But you know what? Now, you're a public company. It's a really long journey. It's the start of a marathon. Why was L&F such a good fit?

James C. Foster (13:11):
That's how I love that question because a lot of people get it wrong. They think that going public, you're like, "Fantastic. You made it. Congratulations. You're done." We don't view that at all. I mean, this is the start of the next leg of marathon. I like to think about it as an Iron Man. You may be finishing one part of that race to where the first 26 miles is behind you, but you realize that you've got three quarters left.

And so this is a milestone for us. This is a financing. We thought there was a really interesting opportunity given our size and scale and given the size of the problem we're addressing in this market that the capital markets and the capital that you could get through those capital markets made a lot of sense. The board was very supportive and our transaction here is somewhat unique.

We are talking about going public in a really difficult volatile market that we haven't seen in quite some time. Our investors and our board of directors are very supportive of this transaction. They're continuing to roll into this vehicle. And so we look at this as having the opportunity to do something that very few people are trying to do right now.

And I would just say on the process, it takes longer than anybody would think. I mean, to get public for all the right reasons, you have to do a lot of diligence. We've got great advisors and it takes a while to do it the right way, which we are.

We have become an acquisitive platform. IDX is a very strategic partner of ours. They've been a partner for ours for several years. There's a lot of trust built with the organization. When we look at target acquisition companies, the bar is set incredibly high. We look for passionate talent. Passionate human talent will be the longest-term competitive advantage and your highest ROI for any organization. And it certainly is at ZeroFox.

And so we came together last year now and said, wow, think of the things we could do together, really owning the end-to-end external cybersecurity market space if we were to put the two organizations together. Your CEO, Tom Kelly, and I sat down and strategized how we would accomplish this. I think we've got the right plan in place.

And now we're just going through the final processes here to get out and put the two organizations together and allow us to offer a broader value proposition to our customers. Everything from pre-breach intelligence and protection through breaches that will happen and then the required responses thereafter, and that's what ZeroFox and IDX will be able to do together that we can't do individually.

Tom Ryan (15:59):
Yeah. So obviously, you're judging threats with AI and analysts and dark web access and breach response and all kinds of things. Cybersecurity was about playing defense for a while. It feels to me like you're almost putting companies on offense with the whole thing, is that the right way to think about it?

James C. Foster (16:18):
I mean, I talk about the time for sitting around and accepting being target practice is over when you work with ZeroFox. I mean, it is incredibly frustrating when I get these calls from prospects and the strategies and the recommendations they're getting is, "Oh, bolster your firewall, add this next layer of defense." There is no other modern warfare strategy that talks about just bolstering only your defense while you're accepting the fact that you're going to get attacked over and over.

And that strategy is flawed in part because you're actually providing an AB strategy for the attacker, because they may send 10,000 things at you. And if there is no strategy to raise the cost of that adversary to increase the cost of that attack, then there is no disincentive for them to continue to change tactics. And so we see some organizations that first come to ZeroFox and they're getting hit at rates that would just blow your mind, I mean hundreds of thousands of attacks per week.

And part of our job is to reduce that volume, to rise that cost to the adversary, to help those organizations fight back, to dismantle the infrastructure that's attacking them. And as we do that, we find that they become much more secure because attacks aren't free. It is costly to stand up an infrastructure to attack a company or maybe even a particular cohort of companies. And we work tirelessly for our organizations, making sure that they get attacked less and then those attacks are less successful.

A lot of this industry just focuses on, "Well, we'll make sure that no attack ever gets through," but they don't focus on the point of how do you stop the attacks, not just stop them from being successful. We look at the whole attack life cycle and attack every inch of it.

Tom Ryan (18:04):
Maybe a question for investors or potential investors down the road. When you engage with a company, what's the economic model of your business?

James C. Foster (18:13):
We're an enterprise SaaS company. We're about as boring as it gets when you think about the model that we've created. We followed the Salesforce model like probably most companies out there at this point now. We're in the cloud offer that's up and running 24/7 VR platform. We built a lot of really deep artificial intelligence technology to help do our analytics at scale for our customers. And in general, we bill annually upfront in advance and charge monthly.

Tom Ryan (18:41):
It's a recurring revenue model. You described it as boring, but it makes it a rock solid business, very high recurring revenue. And when you're a profitable business, you can do better by your clients, innovate, all of that stuff.

James C. Foster (18:55):
We are very fortunate to have great predictability. I mean more than 90% of our revenue is recurring in nature. And that allows us to have great insight, predictability and planning on how we want to invest in the future. I mean, that's right. We don't sell any hardware and we're not a perpetual software shop. So, it's all recurring SaaS subscription revenue.

Tom Ryan (19:12):
Another big concern in the market with everything that's happening in the world is some companies are cut off to capital. You're pursuing a transaction that's going to help your balance sheet pro forma for going public with L&F. What does the balance sheet look like, and are you fully funded to execute on your plan for the next few years?

James C. Foster (19:35):
We will be. We've raised $170 million of committed capital in our PIPE. And then on top of that, it's the trust. And our trust was originally $175 million. In general, both of those processes were oversubscribed and the economics have been locked in since December. So I think that gives us a great confidence that we'll have growth capital for quite some time to fuel our innovation and our organic growth and continue to be acquisitive when we see something very strategic and incrementally positive to the business.

Tom Ryan (20:03):
You can't underestimate that in this market. I think a lot of high-growth tech companies are being taken out to the woodshed because massively high valuations and maybe they're cut off for capital. So to be able to get a financing like this done at the beginning of your journey is just absolutely huge for your shareholders.

One question I know you're going to love, maybe you could talk a little bit about your clients. It seems to me you've got the bluest of the blue chip, great companies, multinationals all over the world. Can you comment on your client base?

James C. Foster (20:34):
I mean, we've got several of the Fortune 10. We've got hundreds of customers in the Global 2000 space. We are growing our six-figure customer base at a 50% CAGR the last three years. And so our big customers are getting bigger. And in cybersecurity, it's really a proof point for a couple things when your big customers are getting bigger. It's recognition of the platform and its maturation. And so I'm very proud about what our team has been able to accomplish over the last few years and the recognition of our ASP growing into enterprise play.

It's also recognition, Tom, of the problem that we're solving. When companies spend more on your particular solution set in cybersecurity, that gives credence to the problem and the importance it has for that organization. And so it is something that we track. We track it meaningfully, and our rise in ASP over the last few years continues to show that this is a very important problem for enterprise organizations and they're investing in their programs at an accelerating rate.

The external cybersecurity problem is not going wait anytime soon. It's the thing that continues to keep those CISOs up at night. They're not worried about insider threats like they were 10 years ago. They're worried about somebody that finds that one weak link in their external armor, gets in and starts compromising their network. And our job is to help make sure that day never happens.

Tom Ryan (21:52):
Yeah, it has to be really gratifying because you're actually doing something incredibly important. What do you think the greatest opportunity is for expansion particularly like in vertical markets?

James C. Foster (22:03):
So unfortunately when bad things happen, it's typically good for our business. And there's not a major market that we haven't tapped into at this point with major customers. External cyber attacks don't differentiate between companies and they certainly don't differentiate by where they're located. If you've got a website, if you've got a social media business page, if you email your customers, you can be attacked and ZeroFox can help. And that means we've got millions of potential customers out there to go get over the next few years.

Tom Ryan (22:33):
Like every single business is a potential customer, like every company in the world, which is just incredible. Just something that is top of mind right now is the Russian invasion of Ukraine. In terms of cyber security from your perspective, what is happening there? What are you seeing and is that changing things for you and ZeroFox? What are you seeing with that?

James C. Foster (22:58):
The Ukraine-Russia war is going to be one of these unfortunate times that we remember 10 and 20 years from now and talk about how warfare symmetrical and asymmetrical warfare was changed. When Russia started to invade and even before invading Ukraine, they were conducting massive reconnaissance operations in the cyber field to understand the types of things that they needed to attack. And then the cyber war attacks started even before the land kinetic warfare was kicked off.

And what happened here is Ukraine realized that they were outmatched in sophistication and technology resources to defend themselves. They went online through social media platforms in particular Telegram, their director of digital transformation and technology went out asking for help and published a wish list to the world and said, "This is the way that we could use defensive support, and here's also things that you could do to help us attack."

And so think of that as crowdsourcing cyber warfare. I mean, it's militias that you could hire from hundreds of years ago now being brought into modern warfare on the cyber front. And from what we've seen, it looks like tens of thousands of people engaged in some of these crowdsource initiatives is the best thing that we've seen so far. And we think that'll change warfare for quite some time. When you've got people all around the world joining in to fight and help defend and fight and help attack, it makes it very, very difficult to defend those attacks at scale as well.

And the challenge is everybody is a target now, and I'll give you a couple examples that are very real. So we've seen customers get attacked for leaving Russia. They say that they're pulling out all their businesses and assets from Russia and they're leaving. And so all of a sudden the risk goes through the roof and Russia sympathist groups and kind of their decentralized cyber gangs started attacking those organizations. So, you're not safe if you leave.

We've seen the exact opposite also happen. And so if you decide to stay in Russia and continue to operate, you've got Ukrainian sympathist groups that are out there now attacking you. And so it's a tough world to navigate if you're a CEO and you've had business in Russia because if you've ever done business there, you have no safe space. You stay, you'll get attacked. You leave. You're going to get attacked.

Tom Ryan (25:16):
What I'm hearing from that is every company big or small has to allocate capital to this issue. It's like you said earlier, it's a must have, it's not a nice to have, right?

James C. Foster (25:28):
That's right. I think the security industry has been on defense for way too long, helping people make sure that not a single attack ever gets through. And again, I think the challenge with that is you have to rely and expect perfection. And what we've seen is that's not a realistic stance, and it's not realistic strategy given where we are today. And so we help our customers go back on offense. Like I said, let's reduce the number of total attacks that are coming after you and the job gets easier.

Tom Ryan (26:30):
Welcome to the Arena. We're working really hard to bring you exciting guests and great content. If you found this episode insightful, subscribe to the show on your podcast app and leave us a five-star rating. The more the show grows, the more interesting voices we can have on the podcast and in turn, that should demystify a lot of the stakeholders around public companies and soon to be public companies. Thanks for listening.

I'm your host, Tom Ryan, we'll see you next time back in the arena.

Speaker 3 (27:22):
References to specific stocks are not intended to be recommendations for specific trading behavior. Comments presented on this podcast are intended for informational and educational purposes only, and do not represent opinions or recommendations on whether to buy, sell, or hold shares of a particular stock. All investors are advised to conduct their own independent research into individual stocks before making a trading decision. In addition, investors are advised that past stock performance is no guarantee of future price performance.

* * *

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.

Additional Information about the Business Combination and Where to Find It

As previously announced, on December 17, 2021, L&F Acquisition Corp. ("*LNFA*") entered into a definitive business combination agreement (as amended, supplemented or otherwise modified from time to time, the "*Business Combination Agreement*"), by and among LNFA, L&F Acquisition Holdings, LLC, a Delaware limited liability company and direct, wholly-owned subsidiary of LNFA ("*L&F Holdings*"), ZF Merger Sub, Inc., a Delaware corporation and direct, wholly-owned subsidiary of L&F Holdings, IDX Merger Sub, Inc., a Delaware corporation and direct, wholly-owned subsidiary of L&F Holdings, IDX Forward Merger Sub, LLC, a Delaware limited liability company and direct, wholly-owned subsidiary of L&F Holdings, ZeroFox, Inc., a Delaware corporation ("*ZeroFox*"), and ID Experts Holdings, Inc., a Delaware corporation ("*IDX*"). LNFA has filed with the U.S. Securities and Exchange Commission ("*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 Business Combination Agreement, including the transactions contemplated thereby (the "*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 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 the 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 LNFA

LNFA 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. LNFA 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.