



We are short:

Ticker ZI

Price ~42

Market Cap \$17 Billion

## **ZI Former Employee Reveals the Secret Sauce Is CEO's College Roommate:**

ZoomInfo (ZI) <sup>1</sup> is a SaaS provider that supplies its subscribers with detailed information on potential contacts. ZI claims 95+% of the contact information it sells customers is accurate,<sup>2</sup> giving ZI an advantage over its peers.<sup>3</sup>

ZI would like investors to believe that the secret to its success is "proprietary insights"<sup>4</sup> gained from investments in AI, ML, and "human-in-the-loop solutions."<sup>5</sup> However, the real secret sauce, according to a high-level former employee ("Former Employee A"), is the CEO's college roommate, a real estate broker by trade, who created SGN Database LLC ("SGN").

ZI uses SGN as a pass-through entity to obscure its purchase of (reportedly stolen)<sup>6</sup> granular data on millions of LinkedIn users for pennies on the dollar from a shadowy entity called OxyLeads, which came under scrutiny in connection with an enormous data breach of hundreds of millions of user profiles.<sup>7</sup>

Our opinion is based on extensive investigative research, including conversations with three former ZI employees, a current employee of OxyLeads's successor, Coresignal, and experts with relevant knowledge of the industry. This research has revealed key pieces of evidence that raise significant questions about the legitimacy and legality of ZI's (secret sauce) data acquisition practices:

---

<sup>1</sup> If you are not familiar with ZI, google your name and "ZoomInfo" and you may be shocked by the library of personal information that it has for you. This [webpage](#) is a helpful resource to exercise your right to have ZI delete your personal information.

<sup>2</sup> ZI, 10-K, 2, 2/24/2022

<sup>3</sup> In our interview with Former Employee B, they stated that ZI has the cleanest and most accurate data, "Almost a monopoly."

<sup>4</sup> ZI, S-1, 141, 11/30/2020

<sup>5</sup> ZI, 10-K, 2, 2/24/2022

<sup>6</sup> See Forbes, *One of The Biggest Leaks Ever Exposes Data On 1.2 Billion People*, Lee Mathews <https://www.forbes.com/sites/leemathews/2019/11/22/one-of-the-biggest-leaks-ever-exposes-data-on-12-billion-people> (OxyData's data was found on a public server and that data appeared to have been copied from LinkedIn, we believe OxyData is the same corporate entity as OxyLeads, see infra 16-22)

<sup>7</sup> *Ibid.*

Former Employee A, who was a high-level ZI employee with knowledge of the purchase of the OxyLeads data, stated in an interview that ZI used a pass-through entity, SGN, owned by the CEO's college roommate, a real estate broker by trade, to mask the fact that ZI was purchasing data from OxyLeads.

- OxyLeads came under suspicion for illegitimately scraping private data<sup>8</sup> from LinkedIn when 380 million individual profiles belonging to it<sup>9</sup> were found on a publicly accessible server, and those files were reportedly accurate copies of existing LinkedIn profiles.<sup>10</sup> Former Employee A asserted that ZI turned a blind eye when the data it received from OxyLeads appeared to be hacked and scraped off LinkedIn.

“We asked for data dumps from [OxyLeads], but it’s not the same people every time. I would go to different people and ask ‘What are we looking for this month’, and it aligned with strategic objectives... A lot of it would come from Henry directly or this C-Suite that’s influenced by sales, the Chief Revenue Officer, Chris, etc. What’s the data that has importance? If you think about the beginning of COVID, it went from a situation that went beyond the main office phone at a company, you wanted someone’s desk phone. Then, later on, when everyone started working from home, you wanted their cell phone... they were getting as many of them as possible.”

- According to another former employee, (“Former Employee B”), the use of OxyLeads data was an open secret in some quarters of the company:

“The entire research team knew about the OxyLeads connection, the data analysts... probably 100 out of 1,000 knew about it.”

---

<sup>8</sup> It is important to make the distinction between scraping public profiles, which is currently legal per the *HiQ Labs, Inc. v. LinkedIn Corp* decision, and logged-in scraping of private user profiles, which was found illegal in *Facebook, Inc. v. Power Ventures, Inc.* Logged-in scraping is what OxyLeads appears to have been doing to get detailed LinkedIn profile information.

<sup>9</sup> The article refers to OxyData.io, we believe this is an alter ego of OxyLeads. There is a web of alternate names and successors to OxyLeads, such as OxyData, Coresignal, and Deeptrace, which we attempt to untangle infra 16-22. Generally, we will refer to this entity throughout this report as OxyLeads since that is the name that was familiar to the former employees. There is another entity called OxyLabs which is also [believed](#) to fall under the Oxy-brand umbrella, and a number of people who currently work at the successor company Coresignal, also worked at OxyLabs.

<sup>10</sup> Forbes, *One of The Biggest Leaks Ever Exposes Data On 1.2 Billion People*, Lee Mathews

- Former Employee A maintained that ZI had a contract with SGN to get data from OxyLeads through May 2021, even though OxyLeads [claimed](#) to have terminated services in 2019.



But as we can see, as of today it appears their website is still soliciting business.

- Former Employee A stated that many of the employees harbored serious questions about the legality of the OxyLeads data and the methods used to obtain it:

“There’s no claim that this is kosher. It’s clearly not when we’re jumping through all these hoops, going through the roommate and stuff like that. We clearly know it’s out of bounds.”

- The former employees indicated that the cheap price of the highly valuable data was a sign that OxyLeads was not selling the data with clean hands. When asked if the OxyLeads data likely came from illegal scraping and hacking of LinkedIn, the former employee replied:

“I don’t know what other explanation is possible.”

“[Without OxyLeads], I don’t see how they could get accuracy on that scale of data from the research department or the contributory network.”

- In addition to buying dubious data, ZI also is searching through the emails of millions of people without their consent. In [exchange](#) for free access to its Community Edition version of its product, ZI gets consent from the user to monitor their inbox and search through their contact book and add all of that information to its product, without obtaining the explicit consent of the user’s contacts or email correspondents.

- ZI skirts its legal obligation to notify California and EU residents, who are protected by heightened privacy laws, that it is gathering their personal information by sending notices that overwhelmingly (and likely by design) end up in email spam folders. Although emails from ZI’s main domain name are placed in inboxes at 90%, ZI uses a different domain name for their privacy notification emails that only makes it to the recipient’s inbox 5%-25% of the time.

### **A Former Employee Asserted That ZI Used a Pass-Through Entity Controlled by a College Roommate of the CEO to Conceal Its Relationship with OxyLeads.**

It is our understanding from conversations with Former Employee A, a high-level employee with knowledge of the purchases, that ZI attempted to conceal its relationship with OxyLeads by using a pass-through entity, SGN, controlled by the CEO’s college roommate (Stephen Nilsen) to make the purchase.

A: “The contract with OxyLeads went from my desk to the college roommate. Then, we had a consulting agreement with the college roommate, meaning that that data went directly between ZoomInfo and the college roommate. And what I can presume with a high degree of confidence, is there was never any conversation between me and the college roommate as to what server you’re going to put the data on, which leads me to believe there’s a corner that gets cut. ‘Hey, here’s the data that we need, when we need it by, they send it to you, you send it to us.’ People in the department just knew where to find that data.”

Q: Stephen Nielsen. Just a realtor? No need for the data?

A: “No, nothing, nothing at all.”

A: “I can’t express to you how little Stephen pays attention to what’s going on. We created a contract, payments, and he looks at the dollar amount. I went to our chief revenue officer, and I was like how much do we pay Stephen? I don’t know if it was 10% or \$10,000, but that was the padding on the contract.”

Although we did not call Stephen Nilsen directly and could not find any records to definitively prove he was the CEO’s roommate in college, we were able to independently corroborate much of Former Employee A’s story.

We can confirm that Stephen G. Nilsen attended the University of Nevada – Las Vegas from 2004 to 2006, which overlapped with the CEO Schuck’s 2001 to 2005 enrollment.<sup>11</sup>

In attempting to ascertain how payments might be flowing from ZI to Nilsen to facilitate the purchase of the OxyLeads data, we discovered that Stephen Nilsen founded a company called SGN DATABASE LLC in 2016 where he was the Registered Agent and Managing Member.

*State of North Carolina*  
*Department of the Secretary of State*

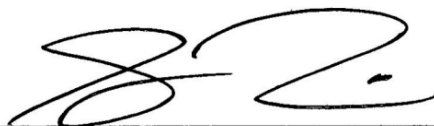
SOSID: 1559230  
Date Filed: 12/8/2016 9:29:00 AM  
Elaine F. Marshall  
North Carolina Secretary of State  
C2016 336 00343

Limited Liability Company  
ARTICLES OF ORGANIZATION

Pursuant to §57D-2-20 of the General Statutes of North Carolina, the undersigned does hereby submit these Articles of Organization for the purpose of forming a limited liability company.

1. The name of the limited liability company is: **SGN DATABASE LLC**  
(See Item 1 of the Instructions for appropriate entity designation)
2. The name and address of each person executing these articles of organization is as follows: (State whether each person is executing these articles of organization in the capacity of a member, organizer or both. **Note: This document must be signed by all persons listed.**)  
STEPHEN NILSEN [REDACTED] (ORGANIZER AND MEMBER)  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_
3. The name of the initial registered agent is: **STEPHEN NILSEN**

This is the 6 day of OCTOBER, 2016.



Signature

**STEPHEN NILSEN, MANAGING MEMBER**


Type or Print Name and Title

<sup>11</sup> <https://www.linkedin.com/in/stephengnilsen/>

As such, we believe that SGN DATABASE LLC, where SGN appears to stand for Stephen G. Nielsen, was the entity through which ZI funneled money for OxyLeads' LinkedIn profiles.

From SGN's annual report in 2017 and their annual report for 2020, we can see that Stephen Nilsen transferred these titles to his wife, Ashley Nilsen, and that the company specializes in data services.<sup>12</sup>

SOSID: 1559230  
Date Filed: 7/17/2017 11:59:00 PM  
Elaine F. Marshall  
North Carolina Secretary of State  
CA2017 198 00997

 LIMITED LIABILITY COMPANY ANNUAL REP

NAME OF LIMITED LIABILITY COMPANY: SGN DATABASE LLC

SECRETARY OF STATE ID NUMBER: 1559230 STATE OF FORMATION: NC

REPORT FOR THE YEAR: 2017

**SECTION A: REGISTERED AGENT'S INFORMATION**

1. NAME OF REGISTERED AGENT: ASHLEY NILSEN

2. SIGNATURE OF THE NEW REGISTERED AGENT: *Ashley Nilsen*  
SIGNATURE CONSTITUTES CONSENT TO THE APPOINTMENT

3. REGISTERED OFFICE STREET ADDRESS & COUNTY  
[REDACTED]

4. REGISTERED OFFICE MAILING ADDRESS  
[REDACTED]

**SECTION B: PRINCIPAL OFFICE INFORMATION**

1. DESCRIPTION OF NATURE OF BUSINESS: Data Services

Filing Office Use Only  
 Changes

<sup>12</sup> [https://www.sosnc.gov/online\\_services/search](https://www.sosnc.gov/online_services/search)



LIMITED LIABILITY COMPANY ANNUAL REPORT

NAME OF LIMITED LIABILITY COMPANY: SGN DATABASE LLC

SECRETARY OF STATE ID NUMBER: 1559230 STATE OF FORMATION: NC

REPORT FOR THE CALENDAR YEAR: 2020

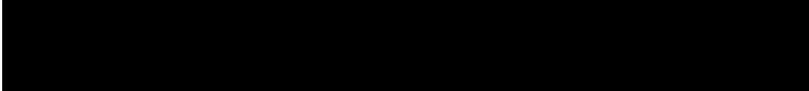
Filing Office Use Only  
E - Filed Annual Report  
1559230  
CA202113104376  
5/11/2021 06:15  
 Changes

**SECTION A: REGISTERED AGENT'S INFORMATION**

1. NAME OF REGISTERED AGENT: Nilsen, Ashley

2. SIGNATURE OF THE NEW REGISTERED AGENT: \_\_\_\_\_  
SIGNATURE CONSTITUTES CONSENT TO THE APPOINTMENT

3. REGISTERED AGENT OFFICE STREET ADDRESS & COUNTY 4. REGISTERED AGENT OFFICE MAILING ADDRESS



**SECTION B: PRINCIPAL OFFICE INFORMATION**

1. DESCRIPTION OF NATURE OF BUSINESS: Data Services

**SECTION C: COMPANY OFFICIALS** (Enter additional company officials in Section E.)

NAME: Ashley Nilsen NAME: \_\_\_\_\_ NAME: \_\_\_\_\_  
TITLE: Managing Member TITLE: \_\_\_\_\_ TITLE: \_\_\_\_\_

We can also confirm Former Employee A's contention that Stephen is a real estate broker by trade,<sup>13</sup> it appears that both Stephen and his wife have a successful brokerage in North Carolina.<sup>14</sup>

<sup>13</sup> <https://stephennilsen.exprealty.com/blog.php>

<sup>14</sup> <https://www.zillow.com/profile/steven8851>

North Carolina - Greenville - Stephen Nilsen



Lead of Steve and Ashley Nilsen

## Stephen Nilsen

EXP Realty

★★★★☆ 4.9 • 8 Reviews

34 sales in the last 12 months

### Our Members



Ashley Nilsen

4.0 ★

1 review

### About us

**Real Estate Agent**

**Specialties: Buyer's agent, Listing agent, Relocation, Foreclosure**

Steve understands first hand that the home buying and selling process can be a stressful one, but it is his goal to make it as simple as possible by guiding his clients each step of the way with his expertise, contacts, and strong negotiating skills.

We were unable to find any other currently operating public-facing businesses they own that specialize in "data services".<sup>15</sup> In fact, when we look at Stephen Nilsen's LinkedIn profile, it he completely omits any mention of SGN, a curious omission for someone who has secured a lucrative contract with a prominent public company.<sup>16</sup>

---

<sup>15</sup> Stephen Nilsen appears to have had several earlier iterations of SGN and related data/profile broking entities that may have served similar purposes as SGN. These other similar entities have all either been dissolved or had their registrations revoked.

<sup>16</sup> <https://www.linkedin.com/in/stephengnilsen/>



 Stephen N.  
Realtor at Steve and Ashley Nilsen Team - eXp Realty

## Experience



### Realtor

Steve and Ashley Nilsen Realtors - eXp Realty  
May 2020 - Present · 2 yrs 2 mos  
Greenville, North Carolina, United States



### Realtor

Steve and Ashley Nilsen Realtors - Keller Williams Points East  
Mar 2019 - May 2020 · 1 yr 3 mos  
Greenville, nc

Steve first obtained his Real Estate license in 2002 after relocating to the Greenville Area from Seattle. Steve holds a Bachelors Degree in History as well as a Bachelors Degree in Social Sciences and a Master: ...see more



### Realtor

Lee and Harrell Real Estate Professionals · Self-employed  
May 2018 - Mar 2019 · 11 mos  
Greenville, North Carolina Area



### Sales and Retention Contact Center Manager

CenturyLink · Full-time  
Jan 2016 - Feb 2018 · 2 yrs 2 mos  
Tarboro, North Carolina



### Managing Partner

BoothCrawler  
2012 - 2015 · 3 yrs 1 mo  
Morehead City, NC

According to Former Employee A, ZI had a contract through SGN to get OxyLeads data through May 2021. When we attempted to corroborate the existence of the contract with SGN with a ZI representative, they tried to avoid the question and then ended up providing a non-denial denial of any relationship with SGN. Apparently, the Nilsen's seem to be taking the same stance, since they don't mention or advertise SGN anywhere we could find.

There is no reason for the CEO, Schuck, to use a personal connection outside the company to create a pass-through entity for the purchase of data from a vendor, unless the point was to conceal the true origin of the data.

It seems as if SGN was barely even a veiled facade over this transaction with OxyLeads, as Former Employee A indicated that people in ZI's research department completely disregarded SGN as a vendor after payment was made and dealt directly with OxyLeads.

Additionally, the former employees dropped all pretenses and exclusively referred to OxyLeads as the source of the data they worked with and never referred to SGN contributing anything more than plausible deniability.<sup>17</sup>

## **Meet OxyLeads: The Shady Data Company That ZI Does Not Want Anyone to Know About**

OxyLeads claims that its services have been terminated since 2019, yet the company's [website](#) invites visitors to contact them if they want to do business.

Hello,

Please be aware that Oxyleads.com services have been terminated since September 25th, 2019.

If you are looking to obtain business professionals (380M+) and companies (14M+) in-depth and continuously updated data records, please get in touch by directly emailing us at [sales@oxyleads.com](mailto:sales@oxyleads.com).

Thank you, Oxyteam

It seems that not only would ZI like to hide the existence of OxyLeads, but the team at OxyLeads is also doing their best to obfuscate what they are doing.

If we check the WayBack Machine, we can see that prior to its claimed termination of services, OxyLeads held itself out as a full-service provider of professional profiles allowing clients to "get practically anyone's business email address":<sup>18</sup>

One reason OxyLeads may want to operate in the shadows is that it appears it was a LinkedIn scraper of dubious legality, as we learned when it was revealed when 380 million profiles they had gathered were left on a public server in one of the

---

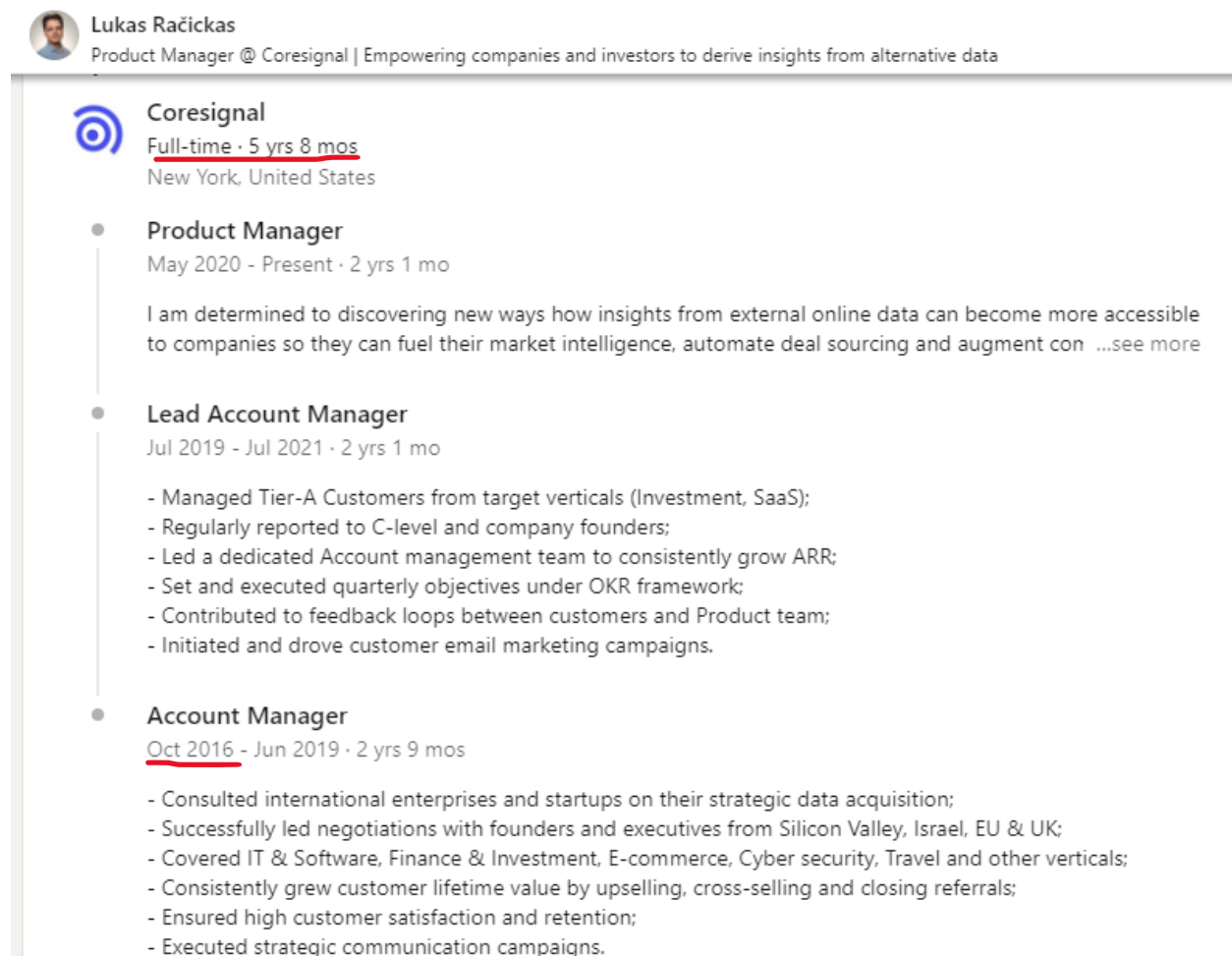
<sup>17</sup> We will carry on with this practice and refer to OxyLeads as the source of the data for the convenience of the reader; however, the reader should be aware that technically SGN is the source of the data since that was the conduit through which the data was purchased.

<sup>18</sup> Wayback Machine, [https://web.archive.org/web/20180115000000\\*/oxyleads.com](https://web.archive.org/web/20180115000000*/oxyleads.com)

biggest data leaks of all time.<sup>19</sup> These profiles were reportedly copies of data from LinkedIn.<sup>20</sup>

As we detail infra p 16-22, instead of really terminating services, we believe that OxyLeads has rebranded as a company called Coresignal.

There are many connections between OxyLeads and Coresignal. Take Lucas Racickas for example, Former Employee A stated that Racickas was ZI's contact at OxyLeads. Racickas' LinkedIn profile states that he has been an employee of Coresignal since 2016.<sup>21</sup>



**Lukas Račickas**  
Product Manager @ Coresignal | Empowering companies and investors to derive insights from alternative data

**Coresignal**  
Full-time · 5 yrs 8 mos  
New York, United States

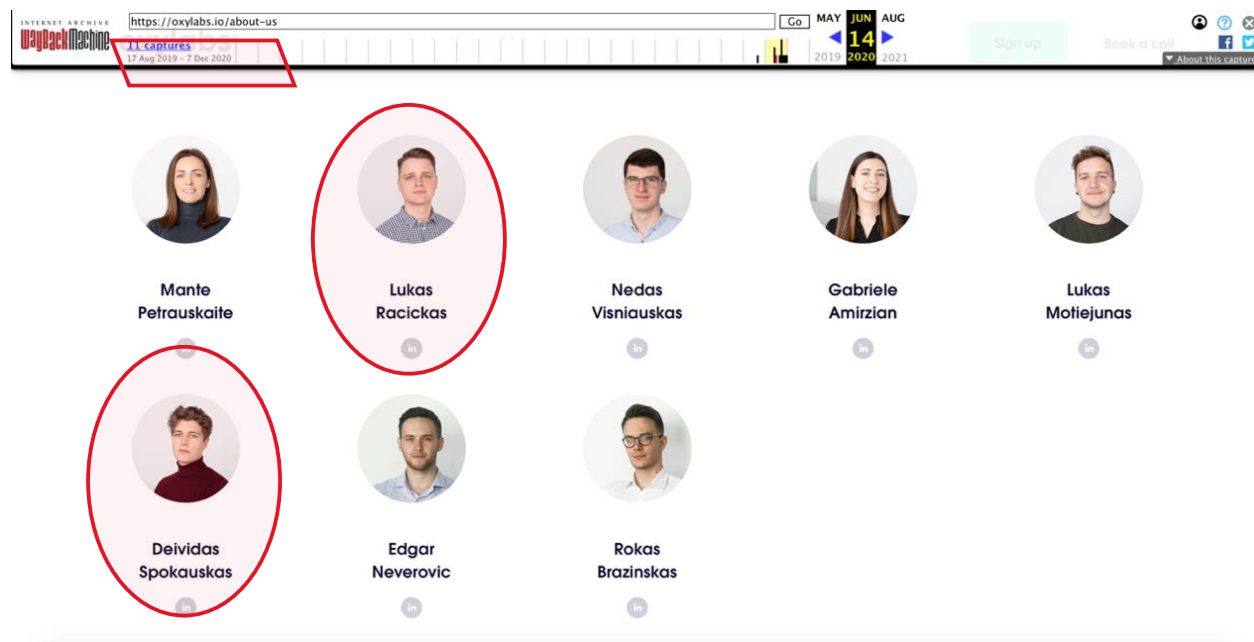
- Product Manager**  
May 2020 - Present · 2 yrs 1 mo  
I am determined to discovering new ways how insights from external online data can become more accessible to companies so they can fuel their market intelligence, automate deal sourcing and augment con ...see more
- Lead Account Manager**  
Jul 2019 - Jul 2021 · 2 yrs 1 mo
  - Managed Tier-A Customers from target verticals (Investment, SaaS);
  - Regularly reported to C-level and company founders;
  - Led a dedicated Account management team to consistently grow ARR;
  - Set and executed quarterly objectives under OKR framework;
  - Contributed to feedback loops between customers and Product team;
  - Initiated and drove customer email marketing campaigns.
- Account Manager**  
Oct 2016 - Jun 2019 · 2 yrs 9 mos
  - Consulted international enterprises and startups on their strategic data acquisition;
  - Successfully led negotiations with founders and executives from Silicon Valley, Israel, EU & UK;
  - Covered IT & Software, Finance & Investment, E-commerce, Cyber security, Travel and other verticals;
  - Consistently grew customer lifetime value by upselling, cross-selling and closing referrals;
  - Ensured high customer satisfaction and retention;
  - Executed strategic communication campaigns.

<sup>19</sup> See Forbes, *One of The Biggest Leaks Ever Exposes Data On 1.2 Billion People*, Lee Mathews <https://www.forbes.com/sites/leemathews/2019/11/22/one-of-the-biggest-leaks-ever-exposes-data-on-12-billion-people>. The article refers to OxyData.io as the possessor of the professional profiles, but as we will explain infra 16-22, we believe OxyData is an alter ego of OxyLeads.

<sup>20</sup> *Ibid.*

<sup>21</sup> <https://www.linkedin.com/in/lukas-racickas/>

However, Coresignal’s parent company Deeptrace Inc was incorporated in 2019<sup>22</sup>. An archived version of the Team page for Oxylabs indeed lists Racickas, although Racickas neglects to mention Oxylabs on his LinkedIn profile.<sup>23</sup>



Racickas was not the only crossover employee; Deividas Spokauskas also pictured above, apparently worked at Coresignal prior to 2019 before its parent company, Deeptrace, Inc, was incorporated.

### **Former Employees Believed That ZI’s Purchase of Data from OxyLeads Was “Super Sketch”**

The only reasonable reason ZI’s CEO would try to hide the purchase of OxyLeads data was if there was something untoward worth hiding. Some former employees harbored suspicions as to the legality of the data. Former Employee A maintained that “The OxyLeads stuff is super sketch” and yet confirmed that purchases continued.

<sup>22</sup> Coresignal is a dba name, the legal name is Deeptrace Inc. Incorporated in Delaware in 2019. See infra 16-22.

<sup>23</sup> We believe Oxylabs is a sister-company to OxyLeads, <https://web.archive.org/web/20200614072232/https://oxylabs.io/about-us>

Q: What makes the data they acquire sketchy?

A: "I'll give you a spectrum. Option 1 – we look at census data. Freely available, you download it and it's done. Option 2 – these FOIA requests. Option 3, we write a script to hit a website to scrape data. It might be a website that has no policy against this. Then, there's a we get a program that creates a little proxy server that allows us to use spiders or agents on the web to mask or change our IP address that may have a policy so they think we have traffic from a bunch of areas when it's really just us." This is a gray area. "Then, there is... OxyLeads had some data, we don't know where it came from, but if we look, there seem to be a bunch of LinkedIn data breaches that seem to be connected to OxyLeads somehow, but we're not going to ask any questions about this, we're not going to ask how OxyLeads got this, but it sure is valuable."

Q: And I'm paying a really cheap price. Is there a shadow of a doubt that it's kosher?

A: "There's no claim that this is kosher. It's clearly not when we're jumping through all these hoops, going through the roommate and stuff like that. We clearly know it's out of bounds."

We infer from this comment that the OxyLeads data was considered problematic because it appeared to have been hacked and illegally scraped off LinkedIn's site.

This data pulled from LinkedIn may have been highly problematic, but it was also immensely valuable because that information comes directly from the data subjects and is the freshest and cleanest source of information available. Since this data was so valuable, it appears ZI just pretended it had no idea that the ultimate source was LinkedIn.

"You have to go back and understand the provenance, the original source of that data. If you look at this People / OxyLeads data breach, the IT press, they're just going to say, I downloaded the data, everything on those LinkedIn profiles matches the data, so they're going to say I assume it's LinkedIn data. But unless you go to that person who pulled the data, I don't think you have any chance of legitimately knowing. And I guess what goes unsaid is, if you don't care, you don't ask."

Former Employee B also understood that the OxyLeads data drew a connection between the information that they were getting from OxyLeads and LinkedIn

Q: Which data sources do they buy from?

A: "One of them that I'm aware of is called OxyLeads. O-x-y-l-e-a-d-s. They provide very similar information to what is on somebody's LinkedIn page. You can't scrape LinkedIn, LinkedIn can't sell data, but OxyLeads provides very similar data to LinkedIn."

"Another is Bombora, b-o-m-b-o-r-a. Bombora provides intent data, like what they're searching."

*As a side note: ZI is currently embroiled in [litigation](#) with Bombora, a company that is suing ZI for unfair business practices.*

Former Employee B didn't just draw a connection between LinkedIn's data and OxyLeads, they harbored serious doubts about the legality of the data.

“Legally, you're not able [to scrape private LinkedIn profiles]. LinkedIn can't sell their data directly to firms, that I'm aware of... OxyLeads is a Ukrainian [sic] firm that I think operates outside of a US jurisdiction, and OxyLeads just scrapes LinkedIn and sells the data to other firms. So they are definitely an offshore firm that gets around the regulations that don't allow US firms to scrape directly.”

Since scraping the public portion of LinkedIn profiles is arguably legal, we can infer that these employees believed that this data either came from illegal data breaches or illegal logged-in scraping of LinkedIn.

In a recent conversation with a current employee of Coresignal, which our research shows us is the successor to OxyLeads, the current employee confirmed that Coresignal has a large infrastructure of proxy servers which it uses to scrape LinkedIn's site.<sup>24</sup>

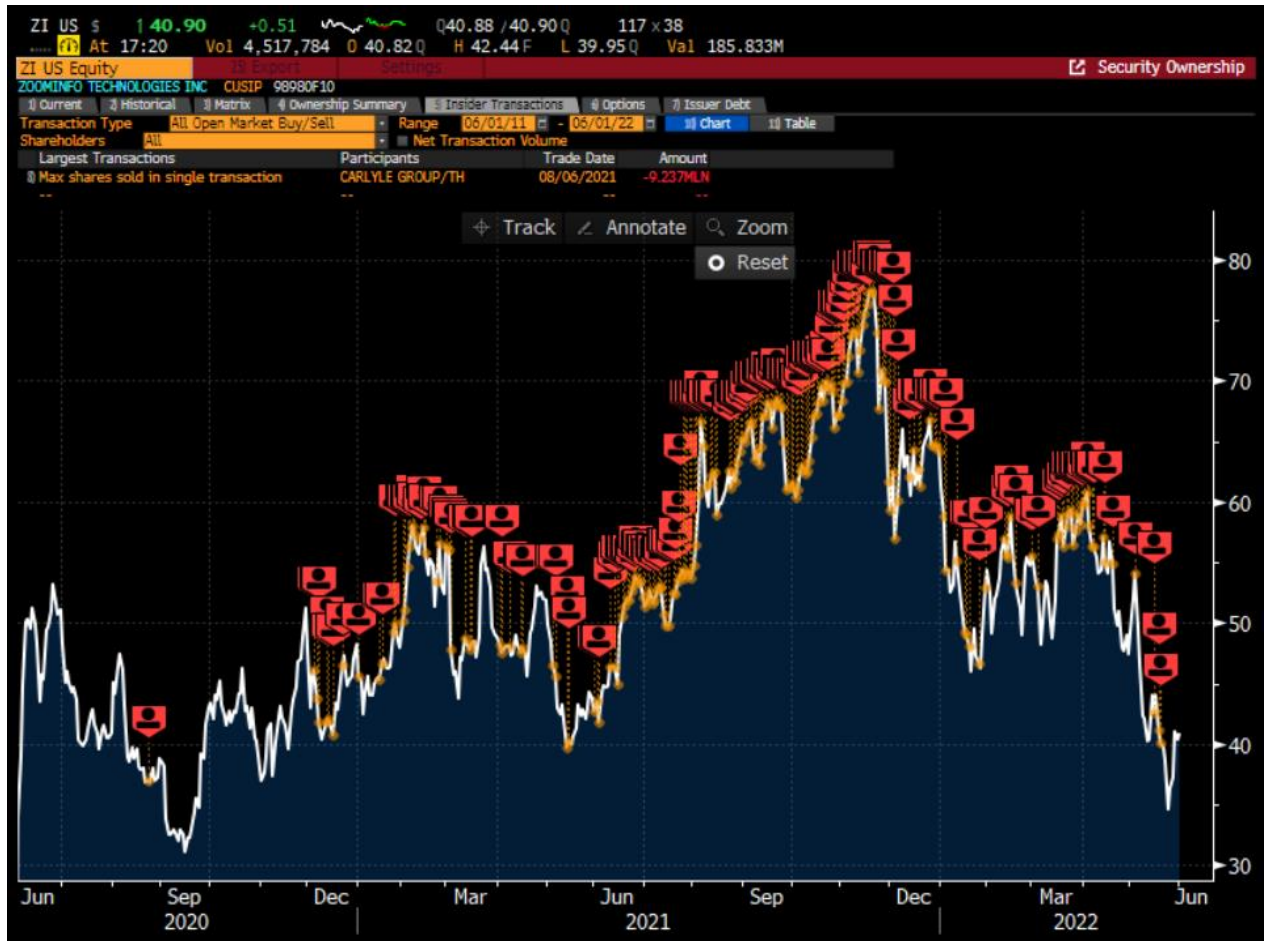
This current employee made a point of stating that the reason their data is so valuable is because it is *current*, indicating that it is continuously scraping LinkedIn. We believe ZI may still be getting LinkedIn data from Coresignal, which our research shows us is OxyLeads' successor.

This use of OxyLeads data could create a major problem with the compliance departments at large ESG funds and other large financial institutions if the data was gathered via logged-in scraping as indicated by the former employees.

---

<sup>24</sup> Once again, we would remind our readers of the distinction between logged-in scraping, which is illegal, and logged-out scraping, which is legal. Unsurprisingly, this employee did not confess to logged-in scraping.

## Meanwhile, the Insiders Have Been Selling Billions of Dollars Worth of Shares



## **In Our View, ZI’s Use of the OxyLeads Data to Plug Holes, and as a Quality Control, Demonstrates Its Technology Claims Are Exaggerated**

We believe that when ZI frames its data aggregation practices, it emphasizes its automated data-gathering and artificial capabilities, while de-emphasizing the role played by third-party data sources: (emphasis added):<sup>25</sup>

We have a number of data sources, including proprietary sources, that enrich our platform:

- **Contributory Network.** Our free users and many of our paying customers contribute data that enhances our platform. Our contributory network captures data on approximately 50 million contact record events daily.
- **Unstructured Public Information.** Our patented and proprietary technologies extract and parse unstructured information found on webpages, newsfeeds, blogs, and other public sources, and then match that information with entities that we have previously identified.
- **Data Training Lab.** We have developed hundreds of processes, largely automated, to gather information from sources, such as PBX directories, website traffic and source code, and proprietary surveys.
- **Generally Available Information.** Our technology adds value to public information and a **limited amount of purchased third-party data** by combining them with our proprietary insights.

ZI frames this use of third-party data as if it is of almost no importance; however, according to Former Employee B it was a key ingredient in the secret sauce, and ZI imported data from Oxyleads every quarter and used it as a quality control:

“Yeah, that’s definitely part of the secret sauce, is that ZI has an entire division called the research division whose primary objective was to find these out-of-the-ordinary data sources that we could check against our database or add information that we didn’t already have in our database. OxyLeads was useful to ZI because of the additional profiles, and then after the ZI acquisition, it became useful because of the education data. [The leader of this research division’s] primary job was to find different data sources from wherever that might potentially add value to the platform. And once you find the data sources, the Research team is tasked with getting them into the data warehouse. OxyLeads is incredibly cheap, because every quarter they would just dump a terabyte of data into a .CSV file.”

---

<sup>25</sup> ZI, S-1, 4, 11/30/2020



Additionally, Former Employee A stated that the OxyLeads data was useful in plugging holes because OxyLeads could vary what data it brought to the table depending on the needs of ZI.

“We asked for data dumps from [OxyLeads], but it’s not the same people every time. I would go to different people and ask ‘What are we looking for this month’, and it aligned with strategic objectives... A lot of it would come from Henry directly or this C-Suite that’s influenced by sales, the Chief Revenue Officer, Chris, etc. What’s the data that has importance? If you think about the beginning of COVID, it went from a situation that went beyond the main office phone at a company, you wanted someone’s desk phone. Then, later on, when everyone started working from home, you wanted their cell phone... they were getting as many of them as possible.”

ZI’s use of this data as a quality control and to plug gaps indicates that it considered the data very reliable, which is peculiar given the method and locus of purchase. The data was certainly not considered reliable because it came from the college roommate of the CEO, or from a company that claims to have shut down operations. The likely reason the data was considered reliable was because ZI verified it was copied from a reliable source, such as LinkedIn itself.

It appears that the quarterly data dumps from OxyLeads played a crucial role in ensuring ZI’s data was superior to its competitors and mirrored LinkedIn’s private database. Access to this private information allowed ZI to offer a product that was more accurate than its rivals, as Former Employee B, stated:

“You just want to be more accurate than publicly available information... ZI is good at being the least inaccurate data source.”

## **ZI’s Purchase of LinkedIn Data from OxyLeads Allowed ZI to Claim High Accuracy Rates**

While it downplays the role of third-party data sources to investors, ZI guarantees to customers that data on the platform will be 95%+ accurate. Per the company’s 2020 S-1:<sup>26</sup>

“Our intelligence is kept up to date in real time. This enables us to provide our customers with a contractual guarantee that at least 95% of the employment information they access will be current. This is accomplished through a combination of robust systems and processes leveraging AI, ML and our proprietary human-in-the-loop approach.”

---

<sup>26</sup> ZI, S-1, 139, 11/30/2020

We understand that ZI views LinkedIn as a competitor. So, ZI's technobabble notwithstanding, it is easy to see why it might be worthwhile for ZI to obtain a copy of LinkedIn's data before inviting any comparisons.

Former Employee A did not believe it would be possible for ZI to maintain their high accuracy rates without the OxyLeads data.

“[Without OxyLeads], I don't see how they could get accuracy on that scale of data from the research department or the contributory network.”

### **ZI's Purchased Data from OxyLeads at Cheap Prices, Providing More Evidence That Suggests the Data was Stolen.**

It appears that ZI was using OxyLeads data as a quality control to assure accuracy and to plug missing data. This bulk data seems to have been the “secret sauce” that enabled the company to have the most accurate and cleanest data.

So how much did ZI spend on these bulk purchases? ZI downplays its reliance on such data by citing decreasing spending (emphasis added):<sup>27</sup>

“We purchase a limited amount of data from third-party vendors (e.g., other data brokers) to be used in our platform. Our technology typically adds value to this data by combining it with our proprietary insights. **In 2019, we spent less than \$3 million on such data, with spend decreasing year over year.**”

When asked about the \$3 million spent on third-party data acquisitions, Former Employee B asserted that only a small portion of that would go to OxyLeads:

“\$3 million seems pretty high to me, because ZI is incredibly good at finding cheap data sources for very little money. OxyLeads every quarter was I think \$100,000 or something like that. Bombora and other I'll call them more legit companies were slightly more a quarter. ZI was very good at finding cheap data... To me, OxyLeads was the least legit because, like you said, regulatory arbitrage. Bombora, Dun & Bradstreet, these are legit data sources where you don't have to call some guy in the Ukraine [sic] to say, hey, what data do you have.”

Since to our knowledge LinkedIn does not sell its private data, and logged-in scraping is illegal, theoretically the only legitimate way to get this private data is to buy the company LinkedIn. In July 2016, [Microsoft](#) put the going rate of LinkedIn at \$26 billion. So, we think that purchasing a copy of LinkedIn's data at \$100,000 a quarter indicates that the data was not legitimately obtained.

---

<sup>27</sup> ZI, S-1, 141, 11/30/2020

Former Employee A also considered the low purchase price as a sign that OxyLeads was not selling the data with clean hands:

A: “The price at which OxyLeads sells the data indicates they are not the genesis of the data. They are just people who package the data out there.”

Q: This is breach data plus scraping?

A: “I don’t know what other explanation is possible.”

## **OxyLeads Operates as a Part of a Shadowy Web of Lithuanian Entities**

As we investigated OxyLeads’ ownership and management, we came upon a chain of increasingly cloak-and-dagger Eastern European data brokers.

There is a myriad of different legal entities in this network, so here is a conceptual framework to help keep things straight. At the heart of this network is a valuable resource, a group of proxy servers that our investigative team believes are in the country of Georgia. These proxy servers, owned by two Lithuanians, have a lot of different potential business applications, both legitimate and illegitimate. The different entities we discuss can be seen as attempts to segregate different applications of these proxy servers.

OxyLeads does not have a listed address on its website, but the Better Business Bureau has a profile for OxyLeads that pinpoints its address to an office building in Manhattan:

**Business Profile**  
**Oxyleads**  
Sales Lead Generation

**Contact Information**

630 3rd Ave Rm 1502  
New York, NY 10017

<https://www.oxyleads.com>

[Email this Business](#)

(877) 529-2503

We believe OxyLeads was originally [registered](#) in Wyoming as OxyData, where it had the same listed address, 630, 3<sup>rd</sup> Ave, Suite 1502, New York, NY, 10017. It shares this address with the person identified as the President/Director, Michael N. Schwartz, a CPA who shares the same address in New York.

OxyData Inc.

This detail reflects the current data for the filing in the system. Print

<b>Name</b> OxyData Inc.	<b>Status</b> ? Inactive - Transfer
<b>Filing ID</b> 2017-000752768	<b>Sub Status</b> ? Archived
<b>Type</b> Profit Corporation - Domestic	<b>Initial Filing</b> 05/05/2017
<b>Standing - Tax</b> ? Good	<b>Inactive Date</b> 01/28/2019
<b>Standing - RA</b> Delinquent	<b>Term of Duration</b> Perpetual
<b>Standing - Other</b> Good	<b>Formed In</b> Wyoming
<b>Fictitious Name</b>	
<b>Principal Office</b> 630 Third Ave. Suite 1502 New York, NY 10017 USA	<b>Mailing Address</b> 630 Third Ave. Suite 1502 New York, NY 10017 USA

Additional Details

History

Public Notes

Parties

Michael N Schwartz (President / Director) Organization:  
Address: 630 Third Ave. Suite 1502, New York, NY 10017, USA

In 2019, Schwartz [transferred](#) the registration of OxyData Inc to Delaware, listing his email as [accounting@oxyleads.com](mailto:accounting@oxyleads.com).<sup>28</sup>

<sup>28</sup> Although this form shows Schwartz signed the paperwork in 2018, the Wyoming State documents indicate the transfer occurred in January 2019.

Signature: ✓ Michael Schwartz  
(May be executed by a member, manager, or other authorized individual as set forth in the operating agreement.)

Date: 12/21/2018  
(mm/dd/yyyy)

Print Name: Michael N. Schwartz

Contact Person:

Title: President/Director


Daytime Phone Number: [REDACTED]

Email: accounting@oxyleads.com

(Email provided will filing evidence)  
\*May list multiple email addresses

OxyLeads and OxyData are also tied together by IP data. The IP data marked for OxyData lists oxyleads.com as its website. The mailbox also is [michael@oxyleads.com](mailto:michael@oxyleads.com). The WHOIS search also identifies Michael Schwartz.

### AS33756 – Oxydata Inc.

Country	 United States
Website	<a href="http://oxyleads.com">oxyleads.com</a>
Hosted domains	0
Number of IPs	0
ASN type	Inactive
Allocated	4 years ago on Dec 04, 2017

POCHandle: SCHWA315-ARIN  
IsRole: N  
LastName: Schwartz  
FirstName: Michael  
Street: 1621 Central Ave  
City: Cheyenne  
State/Prov: WY  
Country: US  
PostalCode: 82001  
RegDate: 2017-11-22  
Updated: 2022-04-05  
OfficePhone: +1-703-925-6999  
Mailbox: michael@oxyleads.com  
Source: ARIN

---

Schwartz may have transferred the registration to Delaware in early 2019 because he may have been under investigation by the DOJ at that time concerning certain tax shelters he had set up for clients. On August 12<sup>th</sup>, 2019, the DOJ issued an [injunction](#) against Michael N. Schwartz, barring him from organizing, promoting, or selling abusive tax shelters.

OxyData/OxyLeads also appears to be [tied](#) to another company, called [OxyLabs](#). OxyLabs allows clients to use their proxy server network to conduct their own scraping projects.

We believe that OxyLeads now has a successor, Deeptrace Inc., whose website is <https://www.coresignal.com>.<sup>29</sup> Deeptrace's records in the Data Broker Registry for the Office of the Attorney General of California indicate it shares the same New York address as OxyLeads, OxyData and Michael N Schwartz.

---

<sup>29</sup> <https://oag.ca.gov/data-broker/registration/192449>

## Data Broker Registration for Deeptrace Inc.

**Data Broker Name:**

Deeptrace Inc.

**Email Address (Accessible to the public):**

[privacy@coresignal.com](mailto:privacy@coresignal.com)


**Website URL:**

<https://coresignal.com/>

**Physical Address:**

630 Third Ave. Suite 1502  
New York, NY 10017  
United States

Coresignal holds itself out as a data broker. Coresignal’s contact information lists the same address as Deeptrace, and its Terms & Conditions page refers to Deeptrace LLC, a Delaware company:<sup>30</sup>

	Use cases	Company	Contact us
	Investment intelligence	About us	630 Third Ave. Suite 1502,
	Trend forecasting	Blog	New York NY 10017
	Data-driven recruitment	FAQ	USA
	Lead generation	Privacy policy	<a href="mailto:sales@coresignal.com">sales@coresignal.com</a>
		Terms and conditions	

<sup>30</sup> <https://coresignal.com/terms-and-conditions/>

**Company** (referred to as either "the Company", "We", "Us" or "Our" in this Agreement) refers to Deeptrace LLC, 16192 Coastal Highway, Lewes, Delaware 19958, County of Sussex, USA.

It appears the owner of Oxydata Inc., became Deeptrace, which does business as Coresignal, making Coresignal the direct successor to OxyLeads.

## **ZI Skirts Privacy Laws by Emailing its Privacy Notifications from a Domain Name That Gets Marked as Spam**

Under the [CCPA](#), ZI has an obligation to notify California residents when it collects their records, and ZI must tell them what it plans to do with that information:

(b) A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used.

ZI must comply with even more stringent rules in Europe under the GDPR, which generally requires that every person provide consent for their personal data to be lawfully processed.<sup>31</sup> The consent must be requested in language that is clear and unambiguous.<sup>32</sup>

ZI appears to have found a way to argue that it is complying with this obligation to notify people that it has gathered their information while still leaving most people unaware of what ZI is doing.

ZI has been able to accomplish this sleight of hand by using a separate domain name when sending out the privacy notification emails that inform people that ZI has captured their data and that they can opt out. With the alternative domain name, the vast majority of the emails are classified as spam and never get placed in a person's inbox.

We can see that several colleges and Universities, including [George Mason University](#), [Clemson](#), [Brown](#), and [Hamilton](#) received the privacy notifications from

---

<sup>31</sup> GDPR Article 6 (a).

<sup>32</sup> GDPR, Recital 39.



domains like "m.zoominfo-privacy.com" and marked these privacy notifications as spam or phishing attacks.<sup>33</sup>

We have seen an email optimization platform test comparing the inbox placement rates of emails sent from the "zoominfo.com" with "m.zoominfo-privacy.com" and the difference was striking.

Messages sent from the "zoominfo.com" domain name had a very high placement in the recipient's inbox, over 90%.

However, emails sent from "m.zoominfo-privacy.com" had an inbox placement that varied from 5%-25%.

Since ZI knows how to ensure its normal emails get placed in the recipient's inbox, it is clear to us that these privacy notifications are getting sent directly to the spam box because ZI does not want people to see them.

It remains unclear if this practice will be considered sufficient to comply with California law, but it seems to fall far short of the GDPR.

Generally, under the GDPR, a person must provide their clear and unambiguous consent if a company wants to process their personal information.<sup>34</sup> Consent must be clear and unambiguous, "Silence, pre-ticked boxes or inactivity should not therefore constitute consent."<sup>35</sup>

ZI claims that it is GDPR compliant, as it earned GDPR [approval](#) from TrustArc, a privacy compliance firm which has given ZI its seal of approval. ZI must have posited some other legal justification apart from consent to legally justify their data processing practices; regardless, ZI still has a legal obligation to be transparent with the people whose data it sells.<sup>36</sup> The GDPR specifically states that transparency requires that "any information and communication relating to the processing of those personal data be easily accessible and easy to understand..."<sup>37</sup> We do not believe that ZI's practice of sending out emails from a domain name that overwhelmingly ends up in the recipient's spam folder is sufficiently transparent to comply with the GDPR.

Violations of the GDPR can result in harsh penalties. The amount is €20 million (\$21.3 million) or 4% of global turnover, whichever is greater.<sup>38</sup> For ZoomInfo, being fined for a breach of GDPR could amount to a significant penalty.

---

<sup>33</sup> People have also expressed their confusion about these missives on [public forums](#).

<sup>34</sup> GDPR, Article 6 (a), Recital 32.

<sup>35</sup> GDPR, Recital 32

<sup>36</sup> GDPR, Article 14

<sup>37</sup> GDPR, Recital 39

<sup>38</sup> GDPR, Article 83 (5)

## **ZI Scrapes Through Its Users' Contact Lists Without Those People's Knowledge or Consent**

ZI offers a free service called Community Edition, which allows users access to their B2B contact lists, in exchange for providing [permission](#) for ZI to scrape their inbox and contact book for contact information. ZI does not just scrape all information on the person who signed up, it scrapes information on every contact and every person who emails the user as well.

In exchange for your use of Community Edition, you agree to let us access information in your email inbox, specifically the information in signature blocks of emails you have received, metadata from email headers, and your contacts in your email contact book.

This means that if you are in email correspondence with someone who signed up for ZoomInfo's Community Edition, ZI is scraping your emails for information about you.

Not only does this raise privacy concerns for ordinary people, it raises significant red flags for lawyers, accountants, and other business professionals who deal with confidential information. ZI's scraping tools have already resulted in the unintended capture and dissemination of confidential or privileged information.<sup>39</sup>

ZI calls this method of capturing information its "contributory network," and consists of paying users and Community Edition users. In 2020 ZI stated its contributory network "captures data on approximately 50 million email signatures, email deliverability, and contact update records daily."<sup>40</sup>

When ZI made this disclosure in 2020, it had 220,000 paying users and an undisclosed number of Community Edition members.

ZI's [terms of service](#) clearly tell its Community Edition users that it intends to scrape the users email information for information from their email, such as:

name, email address, job title, department, company name, phone numbers, business address(es), website URLs, metadata from email headers, and other similar business-related information (collectively "**Contact Data**") that may be stored in your email account both locally or on a remote server.

The user consents, but the people who correspond with these users are also getting their information scraped, and they haven't consented to anything. This lack of

---

<sup>39</sup> As detailed on page 234 of this [PDF](#) (an aggregated record of some comments submitted to the California Privacy Protection Agency by The Sege Law Practice).

<sup>40</sup> ZI, S-1, 1, 11/30/2020

consent is at the heart of the unfair business practices [lawsuit](#) filed against them by Bombora.

It is too early to tell if this practice will be found to run afoul of the EU's GDPR or California's CCPA. But in our opinion, if these laws do not prevent this underhanded method of data gathering, then these privacy laws aren't worth the paper they are written on.

## Financial Disclaimer

Please be advised that WPR, LLC, Wolfpack Research (WPR) is a research and publishing firm, of general and regular circulation, which falls within the publisher's exemption to the definition of an "investment advisor" under Section 202(a)(11)(A)–(E) of the Securities Act (15 U.S.C. 77d(a)(6) (the "Securities Act"). WPR is not registered as an investment advisor under the Securities Act or under any state laws. None of our trading or investing information, including the Content, WPR Email, Research Reports and/or content or communication (collectively, "Information") provides individualized trading or investment advice and should not be construed as such. Accordingly, please do not attempt to contact WPR, its members, partners, affiliates, employees, consultants and/or hedge funds managed by partners of WPR (collectively, the "WPR Parties") to request personalized investment advice, which they cannot provide. The Information does not reflect the views or opinions of any other publication or newsletter. We publish Information regarding certain stocks, options, futures, bonds, derivatives, commodities, currencies and/or other securities (collectively, "Securities") that we believe may interest our Users. The Information is provided for information purposes only, and WPR is not engaged in rendering investment advice or providing investment-related recommendations, nor does WPR solicit the purchase of or sale of, or offer any, Securities featured by and/or through the WPR Offerings and nothing we do and no element of the WPR Offerings should be construed as such. Without limiting the foregoing, the Information is not intended to be construed as a recommendation to buy, hold, or sell any specific Securities, or otherwise invest in any specific Securities. Trading in Securities involves risk and volatility. Past results are not necessarily indicative of future performance. The Information represents an expression of our opinions, which we have based upon available information, field research, inferences and deductions through our due diligence and analytical processes. Due to the fact that opinions and market conditions change over time, opinions made available by and through the WPR Offerings may differ from time-to-time, and varying opinions may also be included in the WPR Offerings simultaneously. To the best of our ability and belief, all Information is accurate and reliable, and has been obtained from public sources that we believe to be accurate and reliable, and who are not insiders or connected persons of the applicable Securities covered or who may otherwise owe any fiduciary duty or duty of confidentiality to the issuer. However, such Information is presented on an "as is," "as available" basis, without warranty of any kind, whether express or implied. WPR makes no representation, express or implied, as to the accuracy, timeliness, or completeness of any such Information or with regard to the results to be obtained from its use. All expressions of opinion are subject to change without notice, and WPR does not undertake to update or supplement any of the Information. The Information may include, or may be based upon, "Forward-Looking" statements as defined in the Securities Litigation Reform Act of 1995. Forward-Looking statements may convey our expectations or forecasts of future events, and you can identify such statements: (a) because they do not strictly relate to historical or current facts; (b) because they use such words such as "anticipate," "estimate," "expect(s)," "project," "intend," "plan," "believe," "may," "will," "should," "anticipates" or the negative thereof or other similar terms; or (c) because of language used in discussions, broadcasts or trade ideas that involve risks and uncertainties, in connection with a description of potential earnings or financial performance. There exists a variety of risks/uncertainties that may cause actual results to differ from the Forward-Looking statements. We do not assume any obligation to update any Forward-Looking statements whether as a result of new information, future events or otherwise, and such statements are current only as of the date they are made.

You acknowledge and agree that use of WPR Information is at your own risk. In no event will WPR or any affiliated party be liable for any direct or indirect trading losses caused by any Information featured by and through the WPR Offerings. You agree to do your own research and due diligence before making any investment decision with respect to Securities featured by and through the WPR Offerings. You represent to WPR that you have sufficient investment sophistication to critically assess the Information. If you choose to engage in trading or investing that you do not fully understand, we may not advise you regarding the applicable trade or investment. We also may not directly discuss personal trading or investing ideas with you. The Information made available by and through the WPR Offerings is not a substitute for professional financial advice. You should always check with your professional financial, legal and tax advisors to be sure that any Securities, investments, advice, products and/or services featured by and through the WPR Offerings, as well as any associated risks, are appropriate for you. You further agree that you will not distribute, share or otherwise communicate any Information to any third-party unless that party has agreed to be bound by the terms and conditions set forth in the Agreement including, without limitation, all disclaimers associated therewith. If you obtain Information as an agent for any third-party, you agree that you are binding that third-party to the terms and conditions set forth in the Agreement. Unless otherwise noted and/or explicitly disclosed, you should assume that as of the publication date of the applicable Information, WPR (along with or by and through any WPR Party(ies)), together with its clients and/or investors, has an investment position in all Securities featured by and through the WPR Offerings, and therefore stands to realize significant gains in the event that the price of such Securities change in connection with the Information. We intend to continue transacting in the Securities featured by and through the WPR Offerings for an indefinite period, and we may be long, short or neutral at any time, regardless of any related Information that is published from time-to-time.