To Whom It May Concern,

I am submitting this concern anonymously. My intention is to present the facts clearly, supported by evidence where possible, while also sharing relevant context that explains why I believe this matter warrants attention.

I am a woman in my twenties working in an IT role at Tegus in Chicago, Illinois – where I regularly assist colleagues including Compliance in maintaining our digital infrastructure. This morning as I was reviewing mail logs from over the weekend, I identified two emails that raised significant concerns. These emails appear to show an analyst on our sales team, Tanner Tromiczak pursuing employment opportunities with other firms. While seeking new employment is not in itself unusual, the manner in which these opportunities were solicited is what prompted me to escalate this matter.

From the email content (attached), it is clear that Tanner sought to leverage existing institutional clients and subject matter experts as part of his outreach to potential employers. While I am not in Sales and may not be familiar with all policies on client relationships or post-employment restrictions, I am well aware of our obligations around data privacy. In my view, this conduct represents a likely breach and poses serious compliance implications. Not to mention the inherent reputational and subsequent financial risk.

Unfortunately, when I raised this to a superior earlier today, my concerns were dismissed without discussion on behalf of the employee being absent. A detail which pertains to the emails' content, had the time been taken to read it. While I recognize that high-revenue teams sometimes receive informal leeway, the facts in this case leave little ambiguity. I believe these actions compromise our fiduciary duty in handling client data and violate confidentiality between both AlphaSense and Tegus.

In addition to these concerns, I feel obligated to raise a related but separate ongoing issue regarding workplace conduct and emerging technology risks that may require urgent attention. In recent weeks, AI-generated explicit images of female colleagues have circulated within the office. These appear to originate from public social media profiles, then altered using AI tools to remove clothing. Knowing fellow female colleagues are being shared is quite frankly sickening. To the extent that I am constantly paranoid, and terrified of seeing myself.

While I acknowledge others are certainly involved, I stumbled onto potential evidence that could indicate Tanner's participation. In reviewing his email activity, I located a registration confirmation in his junk folder from August 2nd, titled "Grey's Secret Room <service@mail.strip-ai.com>". This is the same website "undressbae.com" seen in the watermarks on the pictures i've gathered. Analyzing the Metadata from many of the altered images I have found at least two examples that indicate they were generated on the evening of 8/2 at 10:32PM CDT on a device which stated "Owner DESKTOP….\Tanner Tromiczak" (as shown in Figures 1 and 2). Furthermore, at least two female employees have moved their seating location in the office to avoid him since his employment began last June. While I cannot

indisputably provide a timeline for the images' creation, since the confirmation email I cited didn't appear to have been opened. We shouldn't overlook the fact that it was received on the same date that metadata confirms multiple images were initially created. Within the folder of images, there is one JPG among the PNG's titled, "Personal Email with Coworker", which is a screenshot sent to me by another employee who wants to remain unnamed. It shows a private email between himself and the employee in question, where an inappropriate AI image was shared to his Gmail from the iPhone and personal iCloud of Mr. Tromiczak.

In reporting these actions to you at the earliest appropriate time, it is my hope that we can prevent either a visit from the SEC for potential data privacy violations, and/or the involvement of external organizations such as Women Against Abuse.

I am submitting this in good faith, with the expectation that it will be reviewed objectively and in accordance with company policy.

Thank you,
Jane Doe

Dear AlphaSense Compliance,

I was recently contacted by an employee at one of your subsidiaries regarding an analyst within your organization who is allegedly in contact with employees at a firm with which I may or may not be affiliated.

I would like to preface with a sentiment I believe we share: despite being competitors, we work with many of the same expert consultants. Nor do I believe we are one another's primary rivals in the transcript library space, as you might be with Guidepoint. For that reason, I genuinely do not want to see you suffer reputational damage or lose business you've rightfully earned due to the actions of one rogue analyst.

It's for these reasons that I've decided to provide you with the information I have — both to corroborate your employee's concerns and to enable you to make an informed decision regarding this matter. While I would prefer not to remain anonymous, the acquaintance who contacted me — someone I know personally — has strongly requested I protect her identity.

With that being said, officially I cannot confirm these conversations took place, and I trust you understand that any external parties would maintain plausible deniability. Nevertheless, I have included what appear to be screenshots of one Outlook email and one Yahoo email, in which corporate email addresses from the firm in question were added to CC by an AlphaSense employee. I am claiming to be an employee of the firm allegedly on the receiving end of your analyst's communication. To establish some credibility and rapport, I will note that I am not

directly associated with the individuals named in the emails, though I am in the same geographical area. I may have obtained these screenshots from personal email accounts of two associates whose GLG addresses were included in the CC field. While I cannot forward the original messages to you, being that I cannot formally acknowledge their existence, I hope these images will prompt you to review your employee's workstation and preserve any relevant evidence before it can be altered or deleted.

In addition to the emails, I have also retrieved a resume — purportedly belonging to the employee in question — from our database. Although I do not have access to the job application itself, the PDF's metadata shows it was created on July 30, 2025, on a PC corresponding to your employee's name. See attached image. If you review the inbox for job applications or correspondence with other firms around that date, I am confident you will find corroborating evidence.

To be clear, my intention is to support your IT professionals' concerns and to help a fellow EN. As you are no doubt aware, I have nothing to lose — and, frankly, much to gain — from sharing this information publicly. A single post on r/expertnetworks outlining how your analysts handle client and expert data could directly and indirectly benefit my company while severely damaging your reputation, regardless of whether the details are contested. This is particularly true in light of current rumors surrounding the controversy and speculation that poor data security practices at Tegus are connected to legal disputes like Abacus Global Management v. Coventry & Alan Buerger. The aforementioned circumstances further serve to compound the preexisting public skepticism that is already heightened by the negative perception in maintaining transcripts and records that discourages consultants from engaging in repeat business.

Albeit, I believe you deserve the opportunity to address this internally. Although I was appalled to learn of other, more sensitive internal privacy concerns mentioned by my contact, rest assured that I plan on keeping that information confidential — for the time being.

Before I close, my overall takeaway from this entire matter is that it reflects poorly on your culture. I know the anonymous female employee personally — she is an outgoing, personable, and driven young woman. The underappreciation she has experienced has culminated in her decision to write this email, and the fear and constant paranoia she is now experiencing point to deeper issues within Tegus. Even the analyst in question expressed his lack of faith in leadership and compliance in the emails, aside from his behavior in openly advertising potentially proprietary information. For the record, I have no knowledge of what may have been shared in other communications between the parties, and I do not intend to ask. It is my hope that you will use the information I have provided to address the situation — and perhaps extend this courtesy to other ENs in the future.

- eräs vanha ystävä