IC Everything + Strictly Dark Web

Memorandum

To: All
From: The Office of the CEO
CC: EBLC Advisors

ZOOM
January 20, 2025

IC Everything + Strictly Dark Web
From the Office of the CEO

Esteemed Colleagues,

Congratulations on surviving and thriving in 2024. As of January 22, we expect shareholders and our boards to approve our corporate merger of Strictly Dark Web and IC Everything.

Our Strictly Dark Web (SDW) group has exceeded goals to grow and provide industry leading managed high assurance software development, cybersecurity, and fraud monitoring services. Research firm Gartner has consistently rated our products in the top right quadrant, with highest marks for our product suites in online fraud detection for financial services companies and cybersecurity monitoring for individuals and small businesses. To recap our financials (in case you missed our latest earnings call) over the last year, SDW earned $250 million in revenue (while exceeding our EBITDA goals) for the twelve months ending December 31, 2024, an increase of 20% over 2023 and currently holds $10 million in cash.

We believe there are significant growth opportunities for SDW in cyber threat intelligence and artificial intelligence driven risk management. Our data scientists (working under client funded research projects) have been mining the dark web and the deep web (collectively, the “darknet”). From this obscure environment, we have curated a substantial amount of data about covert networks and individuals located in the United States. We believe this data can be organized, repurposed, and then monetized. We have high hopes for this endeavor, especially with early estimates from our SDW Finance Department of a potential $1 billion in incremental annual revenue for licensing our current database.

Note that we purchased some of this data using bitcoin and also used advanced techniques (AI augmentation, online personas, and access via onion routers) to perform searches. Originally, certain data was encrypted, but our ever so talented data scientists (Lovelace and Babbage) used industry-leading cryptographic analysis tools to decrypt the data into plain text. Once we overcome some legal and technical obstacles, we can begin pitching the licensing of the data to domestic and international government agencies and other ethical companies for use in their fraud and risk monitoring tools to help perform monitoring for their own customer security. Our goal is to take data that may have been available for “bad” reasons and do good - by helping others fight fraud. I mentioned this endeavor to our Legal team briefly at the end of a Zoom meeting and they said something about our purpose being legitimate - so maybe we’re all good? The primary location for our SDW databases are virtual servers located in the various cloud environments.

The specific data set SDW obtained is listed below.

- Full Names
- Physical Addresses
- Email Address
- IP Address
- Phone Numbers
- Passwords
- Last 4 Social Security Number

We may also have limited datasets that include other potentially useful tidbits, like:

- Email and account history

Regarding IC Everything (ICE), over our five-year history as a private equity company, we've consistently met our goals to grow and provide industry leading services in engineering design, research, and offshore manufacturing services. Client surveys and project feedback continue to indicate that we are delivering high quality services and earning our client's confidence and trust. To recap our financials (in case you missed my latest earnings call) in the last year we earned $1 billion in revenue and we hold $200 million in cash.

Several larger clients love our ideas so much that they have expressed interest in investing in our business or participating in a joint venture with us! Most immediately, we intend to explore growth in microelectronics, augmented reality, and multimodal sensors. Our product engineers (working under government funded research projects) have created hardware that allows 2D and 3D data sets to be collected and displayed on glasses (including contact lenses), as well as headsets. From the use of our lenses, we will be able to curate a substantial amount of data about user activity, location, sentiment, and trends to create profiles to support a variety of use cases.

We believe that, through the use of AI, we can better understand a user's location, activities, and intentions. This will allow us to offer a product that provides real-time directions and product offers, assists the visually impaired, supports contact tracing, and augments a user's location with reviews of stores and restaurants they are near. I have high hopes for this endeavor based on a recent podcast I listened to while flying on the Company's private jet from The Disruptors titled "Why Your Eyes Will Soon Have Superpowers". In fact, our ICE Finance Department has early estimates of a potential $10 billion in annual revenue for licensing our future enhanced database. I mentioned this new endeavor to our Legal team during a Microsoft Teams meeting and they said there could be some privacy issues to investigate.

Once we have adequately organized and implemented appropriate security and privacy controls for the lenses and the data we collect and then store, we plan to begin selling the lenses direct to consumers, as well as pitching the licensing of “real estate” in our lenses / user's view to domestic and international ethical companies and possibly government agencies. Our goal is to help people see where they are more clearly and more detailed -- to look up (no longer at their phones), to concentrate and to see a better world! The primary location for our ICE databases are servers located in Santa Clara, California. A multitude of generative AI services may also be added by Engineering shorty.

The specific data our lenses can augment includes:

- Physical locations
- Network IP Address
- Video/photo recordings (primarily for quality control)
- High resolution 3D models (with lidar generated point clouds)
- User profile creation and configuration details
- Mobile device IDs (of connected devices)
- User biometrics, usage, and behavior patterns
- Voice profiles and sentiment analysis

Recipients of this memo are invited to participate in a corporate retreat in Davos next week to contemplate feasibility and risk of our plans from legal, technical, and business perspectives. To this end, we need to specifically answer the following key questions:

(1) which opportunities are most promising and which resources and business assets are most valuable to enable us to move forward? What additional resources are on your wish list?

(2) the legality of potential SDW and ICE projects, and how we can legitimately monetize the data collected, along with sale of related products. Specifically, what are the use cases of how

we can monetize the data in alignment with our company's goals and vision?

(3) what are the data privacy implications that need to be considered?

(4) what are some of the ethical, trust and safety, and reputational/brand impacts to consider? And how do we mitigate them?

(5) how do we structure our product/service and present the data in order to monetize it, including the information asset, formatting, and categorizing (classifying) of the data?

(6) how and where we should store and deliver data, including encryption of the data, who should have access, and hosting ideas?

(7) what security controls should we consider and employ, such as a disaster recovery plan, unauthorized access prevention, and data leak management? Does this change if we add AI RAG services?

(8) how do we manage access to the data in a way to control and limit access on an as-needed basis, and have a tiered permission management model?

Needless to say, this is a highly confidential effort that must be managed with the utmost care and respect for its sensitivity. Please ensure that any member of your team or third -party service providers that works on this effort have executed our company's confidentiality agreement and limit the number of parties engaged in this effort at all times. Also, please create a name for your project team so that we know who's who when you report back with your best ideas. All ideas and questions are welcome.

See you in Davos!