



DataDot Technology Limited

ABN 54 091 908 726

Securities Exchange Announcement

15 April 2013

Response to Media Reports

In reports that appeared in The Sydney Morning Herald and other Fairfax Media publications on 11 April 2013 ("Fairfax Media Reports"), it was alleged that a subsidiary of DataDot Technology Limited ("DataDot"), DataTraceDNA Pty Ltd ("DataTrace"), and the CSIRO had acted inappropriately in characterising its technology and how it was supplied to a major customer three years ago.

DataDot rejects all allegations in relation to the characterisation of its technology. Detail of a proposed internal review in relation to the sourcing of materials and relevant manufacturing details for the major customer are set out later in this release.

DataTrace, now a wholly-owned subsidiary of DataDot, was formed as a joint venture vehicle for the commercialisation of the technology invented and patented by the CSIRO and during the period addressed by the Fairfax Media Reports was owned equally by CSIRO and DataDot. Total DataTrace revenue represented around 10% of Group revenue for the six months ending 31 December 2012.

Confidentiality provisions in customer contracts prevent DataDot from providing details of commercial arrangements with any of its customers. Having regard to that restraint, DataDot advises that:

- An ASX market release on 27 July 2010 announced that DataTrace had been selected by a "European pharmaceutical company to authenticate the entire production volume of one of its most successful drug products" ("European Pharmaceutical Contract"). The value of this contract is far lower than the estimate provided in the Fairfax Media Reports even when aggregated over the contract term.
- The DataTrace security solution is a covert security feature that is invisible and undetectable using low-level security detection methods such as application of UV light or IR detectors. It is applied by customers to their products to validate product authenticity and provenance and to protect product brands against counterfeiting, third-shift manufacturing, grey imports, fraudulent warranty claims and theft.

For personal use only

- The DataTrace security solution is a customised, not a commoditised product offering. Development of the DataTrace security solution for a customer comprises up to five major steps:
 1. Procurement of uncommon ceramic materials containing rare earth compounds that have light-activated properties;
 2. Design and manufacture of these uncommon materials into specific formulations;
 3. Customisation of the formulations for integration into the components used in a customer's manufacturing process;
 4. Customisation of these formulations for application to the customer's product;
 5. Tuning the highly developed DataTrace detection device (the "Reader") to the customised formulations as applied to each individual customer's product using complex and variable detection procedures that rely upon variable algorithms. The Reader has been developed by DataTrace with material investment over a number of years and continues to evolve with technological advances.
- These five elements convert phosphorescent materials into customised, sophisticated spectral fingerprints. In order to counterfeit or reverse-engineer the DataTrace security solution, criminals must mimic not only the formulation process developed by DataTrace but also the customer's production process, as well as having available a detection device with the same capabilities as the Reader. The journalists responsible for the Fairfax Media Reports did not report these components of the DataTrace security solution. Further, the Fairfax Media Reports contain the false claim that in the case of the European pharmaceutical customer single tracers are bought in bulk by DataTrace, re-branded and re-sold to the customer. In fact, DataTrace supplies the European pharmaceutical company a suite of formulations using more than one tracer. The Fairfax Media Reports do not mention the existence of steps 2, 3, 4 and 5 in providing the DataTrace security solution, and in doing so ignored the substantial proprietary intellectual property and value-add contributed by DataTrace in developing the final product. All five development steps were followed in developing a customised security solution for the European pharmaceutical customer.
- The DataTrace customisation process allows customers to configure the security solution that best meets their needs. At the higher end of the security spectrum, DataTrace offers a security solution that has been described by Dr Gerry Swiegers, whose authority in this field is acknowledged in the Fairfax Media Reports, as "central-bank grade security tracer . . . world-class

banknote level security”. Dr Swiegers was employed at CSIRO in developing the technology and subsequently employed by DataTrace in commercialising it until March 2012. To one prospective customer Dr Swiegers wrote: “our [DataTrace] central-bank tracers have typically been developed over many years to be extremely / impossibly difficult to copy or simulate in any way. In effect, they are developed to offer the same, or a better level of protection than would typically be afforded to banknotes in a Western economy by a deep-security covert feature.”

- For some customers, however, this highest level DataTrace security solution will not be appropriate and a lower-level security may be preferred. This may be for cost-benefit reasons or because the customer intends to apply several covert security markers of varying levels of security to their product, and plans to assign the DataTrace formulation to a lower rung in this multi-layer security mix. For industrial bulk materials, where typically a lower level of security is appropriate and requested by the customer, a patented version of the DataDot development process is used. The level of security that best fits the purpose is not necessarily the highest level and most expensive but depends on each customer’s own requirements. The European pharmaceutical company did not purchase a low-level security solution.
- Before executing the European Pharmaceutical Contract, the customer conducted a rigorous product selection process that extended over a period of nearly two years. The process specifically included short-listing and evaluation of potential suppliers, selection of DataTrace as the preferred supplier, customisation of the counterfeit protection system to suit the product security needs of the customer and joint development work with DataTrace. The European pharmaceutical customer was advised by an international consulting company specialising in the provision of advice on the selection and implementation of security solutions to protect against product piracy.
- There has been insufficient time since publication of the Fairfax Media Reports for the Board to establish all of the facts relating to the sourcing of materials and relevant manufacturing details for the European pharmaceutical customer. The difficulty of this task is compounded by the fact that the allegations relate to events some three years ago and the four most senior DataTrace executives who were then responsible for DataTrace sales and company management are no longer with the company. The Board has therefore commissioned DataDot’s General Counsel, with assistance from the Company Secretary, to conduct an investigation into all aspects of the matter and report his findings to the Board. They will have access to all e-mails and

other company records and will confer with staff, former staff if able to do so, the CSIRO and the European pharmaceutical customer if possible.

- DataDot is committed to observing ethical conduct of the highest standard among its employees, contractors and in its dealings with its customers. As a company in the business of anti-theft and counterfeiting prevention and detection, whose people are entrusted with highly confidential customer information and work closely with law enforcement agencies, no lesser standard is acceptable. The Board believes this culture exists within DataTrace today and the company more broadly and remains committed to continued enforcement of this culture throughout the Group.
- The Board is very concerned that the identity of a client and confidential information relating to the company's business affairs has been leaked to the public and serious allegations made about DataTrace management without being given the opportunity to address these allegations prior to publication. The selective leaking of confidential company communications appears to be designed to cause the greatest reputational damage possible to both the CSIRO and DataTrace with reckless disregard for commercial or other broader consequences. These breaches of confidence appear to have been made by a person disgruntled with the CSIRO and do not come from anyone currently employed by DataTrace or DataDot. Nevertheless, the company apologises unreservedly for this breach of confidentiality and reserves its rights against the person causing the breach.

DataDot is an emerging, ethical Australian company developing leading products in the anti-theft and anti-counterfeiting fields which are competing with the best in the world. These products reduce and deter the grave social and commercial ills of theft and counterfeiting in Australia and overseas and make a real difference at the community level where its products assist law enforcement.

Contact Information:

Mr David Symons
Phone 0410 559 184