**Desk Note** (For personal use only and not for distribution) **26th November 2014**

# Nemex Resources (NXR)

| | |
|---|---|
| Price: | 4.5¢ |
| Mkt Cap: | $8.2m |

## Summary Information:

**(as at 26th November 2014 unless otherwise stated)**

**Capital Structure:**

| | |
|---|---|
| Share Price | $0.045 |
| Shares on Issue | 182.2m |
| **Market Capitalisation** | **$8.2m** |
| Cash (June 2014) | $0.8m |
| Options (various prices) | 101.5m |
| Performance Rights | 9.0m |
| 52 week Low/High | $0.071 / $0.012 |

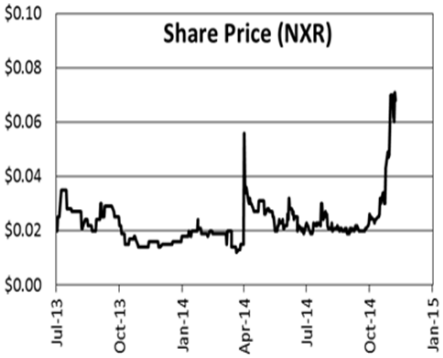
**Directors:**

| | |
|---|---|
| Non-Exec Chairman | Patrick Flint |
| Non-Exec Director | Peter Turner |
| Non-Exec Director | Paul Jurman |

**Major Shareholders**

| | |
|---|---|
| Robert Liu | 13.00% |
| ZhaoQing Dai | 6.25% |

**Historical Share Price:**




## Summary:

### Wavefront Biometric Technologies Pty Ltd

Biometrics is an emerging industry with huge market potential.

Australian-based biometric technology developer, Wavefront Biometric Technologies Pty Ltd (WBT), has developed and patented a unique technology, the characteristics of which gives it a significant competitive advantage over all other forms of biometric technologies. Its highly qualified and experienced development and management team have successfully complete the initial 'proof of concept' development phase as well as the minaturisation of the patented biometric technology technology for reliable and secure authentication of a person's identity to a hand held platform.

WBT is currently focusing on improving the design and performance of the prototype unit, and initiating performance reviews using test groups. Demonstrations of the enhanced product to potential users, as well as the commencement of the commercialisation process, are planned for early 2015.

### Current deal and ownership structure

Nemex Resources Ltd (NXR:ASX) has a 30% interest in WBT. Nemex has entered into a conditional agreement with Wavefront which allows Nemex to earn up to a 51% interest in Wavefront through a series of 4 option payments:

- Tranche 1 (completed) - $0.7m investment for 20%;
- Tranche 2 (completed) - $0.625m investment for further 10% (to 30%);
- Tranche 3 - $1m investment for further 10% (to 40%); and
- Tranche 4 - $1.750m investment for further 11% (to 51%).

The 4 option payments are triggered when phases of development are completed. Completion of each phase entails achieving a set of specific milestones.

NXR has appointed a nominee to the board of WBT and NXR to have pro-rata board representation following completion of Tranche 3 payment.

If NXR fails to complete any of the payment tranches, the agreement is terminated. NXR will retain any interest in WBT that it has earned, and will have first right of refusal over any equity raisings by WBT for the 3 months following termination.

Notwithstanding that the agreement is binding, formal share subscription and shareholders agreements will be entered into to more fully document the funding agreements.

# Key Points:

## The Most Important Security Breakthrough of the 21st Century? We think the 'Eyes' Have it. Well, you only need one of them

Scanning your eye, fingerprint, palm print or face to prove your identity, used to be strictly in the realm of science fiction movies or perhaps even James Bond. Certainly inside the paradigm of daily use in the general population; somewhere well into the distant future.

But in 2014, you can unlock your phone, apartment door, or even start your car using but a fingerprint. Biometrics are now a significant part of our daily lives, and they are here to stay. In fact, it's the PIN code and password that are standing on shaky ground. Are we in the midst of a security revolution?

Like any new technology, there are limitations, even dangers. The global race is on to find most versatile and secure biometric to address some of the greatest challenges of securing the modern financial system.
Perhaps the greatest danger with relying on existing biometrics to secure our personal details and data is called the "Man in the Middle Attack". That's where a 'hacker' sits in the middle between the biometric that secures your data and your data itself. Your security is compromised when the hacker intercepts the transmission of your biometric. The stolen biometric (for example your fingerprint data), gives he or she access to your personal data (such as bank accounts etc) until the breach is discovered.

The 'holy grail' of biometric research and development is the discovery of a biometric that is simple to use, yet so sophisticated that it overcomes the "Man in the Middle Attack".

Wavefront believes it has its foot planted firmly on just such a biometric breakthrough.

Wavefront (of which NXR:ASX is a significant shareholder) believes it is on the verge of a biometric security revolution. A revolution that could yield the holy grail of virtual and real security: the 'One-Time-PIN'. A biometric pin equivalent, so secure that it could make all other biometrics, pin numbers and passwords virtually obsolete and make major inroads into banking/credit card fraud.

A biometric that **renders all stolen personal biometric data useless**.

And it couldn't have come at a more opportune time for the company, as Apple are rolling out Near Field Communication (NFC) into the iPhone 6. NFC allows the phone to be scanned (or vice versa) to make purchases; for example paying your restaurant bill by swiping your phone. This gives grave doubt to the future relevance of "plastic".

The caveat to this, is that for Wavefront to be a commercial success, it doesn't actually need to make all other biometrics obsolete. This is because by overlaying biometrics on top of each other can greatly increase the security when compared to a single line of defence.

One interesting fact about the invention is that it isn't as recent as you might think. It just took certain specific advances in mainstream technology to catch up and allow the breakthrough to be potentially rolled out to a mass market. This major impediment has been mainly the insufficient resolution of the cameras on our smart phone, tablets and PC's to take detailed enough readings of the cornea.

But not anymore.

And of course the processing power of hand-held devices has significantly improved over time which facilitates calculations locally on the handset.

## The Key Feature for Unlocking the Value of the Cornea for Security

The key to the efficacy of this biometric in the field of security is characteristic of our natural 'tear film dynamics'. In layman's terms, your cornea is spherical – movement of the tear film causes variation in the data set every time an image is taken of the eye's surface.

But significantly the variation intra-subject is significantly smaller than the difference inter-subject. While the difference of one data set to another in the same subject is small, the difference between the data set of one subject and a different subject's data set is large. In layman's terms, while your cornea is changing ever so slightly it is significantly different to anyone else's on the planet. For the maths geeks amongst us, this is the perfect environment to construct an algorithm to authenticate identity, which Wavefront has done.

Exhaustive research on a large data base of more than 2,000 subjects for more than 10 years shows no two subjects share the same corneal biometric parameters.

The technology developed by WBT uses the pattern of light reflected back from the contour or topography of the tear film on the corneal surface of the eye as it's biometric. It is also simple to use:

- An illuminated target is reflected off the front of the user's eye and is captured by either a standalone or smart device such as a phone or tablet;
- The pattern of the reflected target that is captured in a digital image depends on the exact shape of the user's eye;
- The captured image is processed to detect the reflected pattern features;
- The detected features are used to enroll or authenticate the user's eye; and
- User enrollment and authentication are quick and simple operations.

## Strengthening the Security of the Data to Avoid Replay Attacks

If a gummy bear and a wine glass can "lift" a fingerprint, what can lift a cornea?

Obviously, it's more challenging to steal a person's eye but it gets better than that. Way better. The corneal biometric is a very rich source of data and lends itself to various methods of utilising the data to strengthen the process of authentication.

Mid-periphery, Central Cornea, Margin of the Cornea; permutations and combinations of these can yield a variety of data sets that when overlayed would further enhance the strength of the application.

"Picture for a second the movie the Matrix and a screen full of columns and rows of numbers that are continually cascading down the screen, each pertaining to different parts and sections of the cornea" says inventor Stephen Mason.

According to Mason, this forms the basis for a "multilayered biometric", and subsequently a multilayered approach to analysis. So, it's not just one algorithm that is protecting your data. It's many. "Trust me, I've had every kind of 'what if' scenario thrown at me over the past 10 years. I've heard them all, and it often still keeps me up late at night. And yet, I still haven't found a single Achilles Heel in this technology".

## How Important will Biometrics be in the Fight Against Fraud and Other Security Breaches?

Biometric technology is slowly spreading across all the industries wherever security is of the prime concern. Biometric technology is largely deployed in the application areas like government, travel and immigration, banking and finance, and defence. Government applications cover voting, personal ID, license, building access, etc.; whereas travel and immigration use biometric authentication for border access control, immigration, detection of explosives at the airports, etc. Banking and finance sector use biometric authentication for account access, ATM security, etc.

## Wavefront's Management

WBT's highly qualified and experienced development and management team includes:

- Dr Shanny Dyer – WBT Chairperson: Extensive experience of technology commercialisation.
- Mr Gary Blair – Consultant: Extensive experience with technology risk and security management. Previously EGM – Cyber, Identity & Privacy at CBA and CTO at NAB.
- Dr Ed Sarver – Co-Inventor: World leader in developing innovative software and hardware for measuring the corneal signal and corneal modelling. Leading the final stages of Wavefront's development strategy.
- Mr Stephen Mason – Inventor: Experienced Optometrist, extensive knowledge of corneal mapping.

## What Have They Achieved?

WBT's technology has demonstrated industry leading-biometric capability when applied via a desk-top device. WBT's objective is to adapt this proven technology to a miniaturised, mobile device. WBT has designed a three phase development program to achieve this objective.

In August 2014, WBT completed the first phase of its technology development program, on time and on budget. This involved WBT successfully miniaturising and adapting its technology to a mobile platform. The basic functionality of the technology on the miniaturised unit was demonstrated, and this included acquiring a live image from the contour of the cornea, enrolling and authenticating the individual, and rejecting an incorrect individual.

WBT's current phase (Phase 2) of development, which is planned to take six months to complete (completion date February 2015), is focusing on improving the design and performance of the prototype unit. This work will include completing a series of performance reviews of the prototype unit using test groups. WBT will produce four prototype units for parallel testing.

## What Does it Mean to the Consumer?

An extraordinarily strong PIN number equivalent for a start. And hence piece of mind.

Imagine, being able to download an application onto your smart phone, that will be able to photograph your eye and use your cornea to determine your identity with 100% accuracy.

Wouldn't that mean all the subsequent purchases you made online using that device using either Near Field Communication (NFC) or online purchases, would be completely secure? Certainly secure in the sense that they have been authorised by you. And you alone. That's powerful.

Would that not put an extra layer of security in defence of your online purchases and therefore make credit card fraud all that much harder? If not impossible and therefore avoid nasty surprises when your credit card details go missing.

The key point is that current biometrics such as fingerprints have major deficiencies. As before mentioned, stealing ones fingerprint is quite conceivable. All it takes is a wine glass and a gummy bear. All the while, finger prints as a biometric are becoming more and more popular. Mainstream even. Take the Apple iPhone 5s for example.

## What Does it Mean to Online Vendors?

A chargeback, also known as a reversal, occurs when a buyer asks a credit card company to reverse a transaction that has already cleared. Theft, and subsequent use, of credit card details is a common reason for chargebacks. 'Friendly fraud' is another common reason for chargebacks, occurring when customers dispute charges that they legitimately incurred. According to a report published by LexisNexis in August, 'friendly fraud' is more prevalent than identity theft.

Online merchants are at greatest financial risk because merchant accounts generally specify that the merchant will be 100% liable for any type of online fraud that might happen. The onus is on merchants to prove that the transaction was not fraudulent which, given current the nature of the online payment process, is very difficult. This leaves merchants at risk of losing products or services that have already been sold, the payment, the fees incurred for payment processing, money for chargeback penalty (up to $100) or even possible commissions for currency conversions. Even if the merchant is able to provide sufficient evidence to support the transaction, the average chargeback process can last anywhere from 75 to 100 days which is time-consuming and expensive for businesses to deal with.

According to LexisNexis, the average merchant lost .68% of annual revenue to fraud in 2013, but the total cost is a multiple of that. For every dollar lost to fraud, merchants spend a further $3.08, to replace lost inventory and cover chargeback fees and other penalties, according to the survey.

According to Matt Barrie of Freelancer (FLN:ASX), "Charge backs are a real problem for Freelancer. I have a whole fraud team. I also have a whole engineering team doing machine learning".

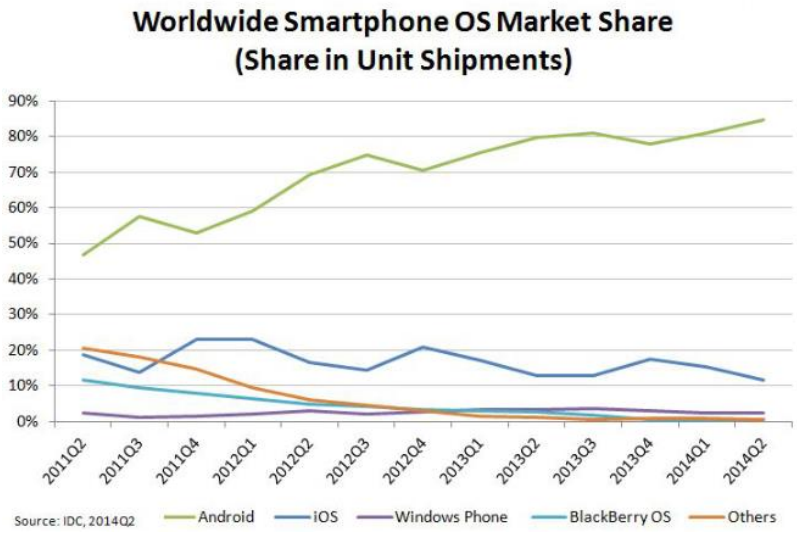
The use of Wavefront technology, in the identification of the cardholder at the point of payment will ease the burden on merchants as the cardholder's unique biometric pattern is required for payment authorisation.

## What Does it Mean to the Major Telco's?

Apple, Google Android, Samsung, Microsoft and Blackberry could all get the edge on each other if they were to own this technology.

Research firm NDP Group's Mobile Phone Track shows that of 121 million smartphones sold in America during 2013, the iPhone accounted for 45%, making Apple the largest smartphone maker in the US. Overall smartphone sales were up 21% year over year.

| US Smartphone Market Share | | |
|---|---|---|
| Brand | Unit share in 2013 | Handsets sold in 2013 (million) |
| Apple | 45% | 54.45 |
| Samsung | 26% | 31.46 |
| LG | 8% | 9.68 |
| HTC | 6% | 7.26 |
| Motorola | 4% | 4.84 |
| Other | 11% | 13.31 |




Looking at operating systems, Android continues to dominate the global smartphone market, with over 255 million units shipped and 84.7% of the market share in the second quarter of 2014. Samsung was the largest vendor of Android-based devices, followed by Huawei, Lenovo and LG. iOS experienced a slight drop in market share, down to just 11.7% from 13.0% in the same quarter last year, representing the growing shift of demand toward low-cost smartphones.

In China, where handsets and tablets are rapidly taking the place of PCs as a consumer' main internet device, "phablets" with screens larger than five inches accounted for 31% of all sales in the three months ended January 2014 according to WPP market research division Kantar Worldpanel ComTech. "Phablet sales across Europe and US have been gradually rising, but it's China which is driving demand," writes Kantar director Dominic Sunnebo. "Phablet owners are less likely than the average consumer to own a tablet, indicating that phablets are increasingly being used as the primary device to browse online in China."

The shifting trend toward the use of phablets as a primary internet device is supported by the figures for internet users who made purchases via a mobile device in June 2013. In China this was 18%, India 15%, Great Britain 10% and Australia and US at 8% each.

This results in consumers demanding an even greater level of security from their mobile devices as they are increasingly used not only as a means of communication, but also to approve online payments, access personal financial data and well as other sensitive information. Manufacturers are left with the task of meeting this demand.

## What Does it Mean to the Security Companies with Security Hardware?

Imagine being Honeywell (NYSE:HON). Or another "large" multinational with deep channels in the security space. (NYSE:HON is currently capped at US$73.19b.)

You already own the hardware that you sell or lease and install to your customers who rely on you for your security needs. Perhaps that hardware already relies on a fingerprint scanner, another biometric. What is stopping you from now strengthening your security system by overlaying it with an additional biometric – the cornea – that doesn't share the same deficiencies that the other biometric(s) are characterised by.

As soon as the customers hear of the strength and validity of Wavefront's cornea breakthrough, they could conceivably encourage or request their security company to adopt the technology and use it as an overlay. In other words, we envisage strong "demand pull" from the Wavefront breakthrough.

Other companies who should have an interest in the technology include 3M, Honeywell and Oracle (NYSE:ORCL).

3M offers a range of biometric products including fingerprint scanners (for use in access control), livescan solutions (for scanning of tenprint and palm print), dual iris scanner (for use in civil registry enrolment, biometric document issuance, applicant identification, border control, and inmate release management).
Its biometric systems are available to governments, law enforcement agencies, and commercial enterprises,

In contrast, Honeywell and Oracle's biometric suits currently appear to be quite limited.

While a search of the security solutions offered via Honeywell's website does show a 'Biometrics' section (which makes reference to combined face and iris recognition systems), the only biometric reader offered seems to be the 'HandKey' (by Recognition Systems Inc.) which maps and verifies the size and shape of a person's hand via measurements such as the lengths, widths, thickness and surface area of the fingers and hand.

Oracle does allows for the integration of biometric scanning systems into its customer solutions (such as the Oracle Access Manager single sign-on) using products such as BIO-key (by BIO-key International Inc.), however the company does not currently seem to own its own biometric reader technology.

## How Big is the Market and Are there any Recent Examples of Security Compromises?

Online fraud is estimated to be costing international banking institutions billions of dollars – each year. Identity theft is the fastest growing crime in the USA. Recent examples of stolen customer records include:

- Adobe (NASDAQ:ADBE) – 152,000,000 records stolen. Hackers obtained access to a large swathe of Adobe customers IDs and encrypted passwords and removed sensitive information (i.e. names, encrypted credit or debit card numbers, expiration dates, etc.).
- Ebay (NASDAQ:EBAY) – 145,000,000 records stolen. The company has said hackers attacked between late February and early March with login credentials obtained from "a small number" of employees. They then accessed a database containing all user records and copied "a large part" of those credentials.
- Target (NYSE:TGT) – 70,000,000 records stolen. Investigators believe the data was obtained via software installed on machines that customers use to swipe magnetic strips on their cards when paying for merchandise at Target stores.
- Home Depot (NYSE:HD) – 60,000,000 records stolen. May be the same group of Russian and Ukrainian hackers responsible for the data breaches at Target, Sally Beauty and P.F. Chang's, among others.
- Korea Credit Union; 20,000,000 records stolen. An employee from personal ratings firm Korea Credit Bureau was charged with stealing the data from customers of three credit card firms. The stolen data includes the customers' names, social security numbers, phone numbers, credit card numbers and expiration dates. In a country of 50 million, this impacted around 40% of the population.

Access to security areas and high value equipment is of critical importance in the defence sector. Recently, Tony Herrin and Devon Biggs (civilian employees at the Sierra Army Depot in Lassen County USA) were indicted for removing U.S. military equipment from Sierra Army Depot buildings, adjusting item codes in the computer database to conceal their thefts and arranging to sell the equipment to various buyers between January and April 2013.

There are also charges against Pedro Luis Infantes and his son, Luis Rafael Infantes, for the theft of government property including 17 military-grade, thermal-imaging monoculars, rifle cleaning kits, and other assorted military equipment for which they attempted to arrange a sale in July 2014.

Security over personal electronic devices is equally important to the average consumer. Recent hackings of numerous iCloud accounts, including high profile celebrities', could be a result of a computer code that repeatedly guesses passwords for Apple's iCloud service until correct, experts say. The script uses the top 500 most common passwords approved by Apple in order to try and gain access to user accounts. If successful, it would give the hacker full access to the iCloud account, and therefore photos. If you think that your password is secure, think again. One commercial software recover program intended for forensic use claims that it can check 2.8b passwords a second.

International airline travel security is another area which is at constant risk of fraud. This was brought to international media attention recently during the investigation of the disappearance of the Malaysia Airlines flight MH370 when it was discovered that two of the passengers were using stolen passports, leaving the world speculating whether the stolen passport holders were terrorists The international policing organisation Interpol says more than a billion travellers last year boarded planes without their passports being checked against its data base of 40 million lost or stolen passports.

## So What is it Worth and Who is it Worth the Most to? Are there any Comparables?

**Recent purchases at a glance**

| Date | Acquired company | Acquiring company | Details | Price |
|---|---|---|---|---|
| Dec-10 | Cogent | 3M (NYSE:MMM) | Cogent develops biometric recognition systems that allow government and businesses to identify individuals by their fingers, palms, faces, and irises. It was purchased to form part of 3M's Security System's Division. | US$943m |
| Jul-11 | L-1 Identity Solutions | Safran (Paris:SAF.PA) | The French aerospace and defense systems company purchased most of L-1, specialising in developing fingerprint, palm, face, and iris biometric recognition solutions. | US$1.09b |
| Jul-12 | AuthenTec | Apple (NASDAQ:AAPL) | The acquisition of the fingerprint sensor technology developer helped Apple attain patents for biometric security in its mobile devices. | US$356m |
| Nov-13 | Validity Sensors | Synaptics (NASDAQ:SYNA) | Acquisition of fingerprint identification firm Validity by the long-time leader in touchscreens has seen its shares double between August 2013 and August 2014. | US$255m |

The acquisition of AuthenTec by Apple also highlights the importance of vertical integration. While Apple clearly benefited from the deal, AuthenTec's other customers, which included Samsung (KSE:005930.KS), HP (NYSE:HPQ), Dell (NASDAQ:DELL), Lenovo (HKSE:0992.HK) and Fujitsu (JPX:6702), were left in a state of panic after being notified that as of 2013, AuthenTec would no longer be honouring orders.

## More on Sales Precedents and Valuation Metrics in the Biometric Space

MasterCard has been researching biometric technologies since 1995. Last month, Nigeria issued the first of its MasterCard-branded eID cards which require Nigerians 16 years and older to provide 10 finger prints, a facial photo, and an iris capture. The card features 13 applications, including MasterCard's prepaid payment technology and Cryptovision's biometric identification technology, providing millions of Nigerian's with the ability to perform safe electronic payments. According to the BBC all Nigerians will be required to have such a card by 2019 if they wish to vote in the country's upcoming elections.

As mentioned earlier, in 2012, Apple purchased the fingerprint sensor technology developer AuthenTec for US$356m, paying a 58% premium for the Melbourne, Florida-based company. Following the announcement, shares of AuthenTec surged US$3.35, or 66%, to US$8.42 on NASDAQ. Apple stock closed up US$10.28 to US$585.16.

Synaptics' US$255m acquisition of fingerprint identification firm Validity Sensors in November of 2013 has seen its shares double in the past 12 months. Fingerprint revenue now accounts for 22% of Synaptics' total sales. Soon after the acquisition, Samsung Electronics struck a deal with Validity to manufacture the fingerprint sensor for its new Galaxy S5 smartphone. According to Synaptics' CEO Rick Bergman, "virtually every mobile customer or PC customer out there is looking at additional biometric or fingerprint solutions."

In June of 2012, social networking giant Facebook announced its acquisition of Face.com, an 11-employee Israeli startup specialising in facial recognition technology, for around US$60m. This was important to Facebook due to the high volume of untagged photos which represent lost opportunities for engagement because when users receive an email notification that they have been tagged in a photo, they probably visit Facebook immediately to check it. These tags also help Facebook understand who a photo is relevant to, so it can feature it in the news feeds of the user's closest friends.

In September, iris recognition company Delta ID announced it has closed a US$5m Series A financing led by Intel Capital and a few strategic investors, bringing Delta ID's total capital raised to date to US$6.1m. The financing will help Delta ID meet the rising demand for its iris recognition products from some of the most high-profile device manufacturers in the world. "We believe biometrics technology will increasingly become a part of how people interact with personal computing and mobile devices, enabling safer, more secure, and convenient user authentication," said Erik Reid, vice president of Intel's mobile and communications group and general manager of its tablet business unit.

CACI International (NYSE:CACI) is a leading provider of biometrics and identity solutions and services, including managed security services, insider threat policy and detection and human entity analytics. A member of the Fortune 1000 Largest Companies and the Russell 2000 Index, its investment in biometrics has served it well, yielding operating income of US$270.8m for the year ended 30 June 2013 and an EPS that has risen from US$4.76 to US$6.18 to US$6.59 over the 2011-2013 financial years. At 6 November 2014, it had a market cap of US$1.99b.

## What Else Lies in Stall for Wavefront?

In the second half of the next development phase, WBT will also commence commercialisation discussions with participants in the financial services and military/defence sectors. This will involve demonstration of the miniaturised prototype in Australia and North America to leading mobile device manufacturers, banks and defence industry groups.

The current prototype is considered appropriate for application in the defence and potentially access control, subject to completion of performance testing and refinement of the design. WBT will seek multi-national companies and Government bodies in the defence sector for licencing agreements. The strategy for commercialisation in the mobile banking sector is to secure a development partner (such as a mobile device manufacturer) for incorporation of the technology directly into a mobile device (software only solution), or as a further miniaturised attachment similar in size to a bank security token.

The incidents mentioned above demonstrate the potential markets for WBT's technology are very significant. PWC UK's 2014 Information Breaches Security Survey indicates that almost three fifths of the respondents are expecting to see more security incidents in the next year with the average cost to a large corporation of its worst security breach for the year is £600k - £1.15m (up from £450 - £850k a year ago) while the average cost to a small business is £65k - £115k (up from £65k a year ago). Considering that the survey also identified that 70% of organisations keep their worst security incident under wraps, what's in the news is just the tip of the iceberg.

## What are the implications for Nemex?

For a strategic investor wanted to get a significant stake into the latest biometric, the simplest and most secret way in is to buy shares into the listed company NXR: ASX who are on target to owning 51% of Wavefront. Once of course, a buyer amasses a holding of 5% they must disclose their shareholding and make a "substantial shareholding" announcement. Currently there are two shareholders that already own more than 5%.

Ian Leete
Investment Manager

Phone: 0415 707 065
ian@altocapital.com.au

# Investment Managers

Adam Belton
Director
Phone: +618 9223 9818
adam@altocapital.com.au

Craig Brown
Director
Phone: +618 9223 9828
craig@altocapital.com.au

Shane Wee
Director
Phone: +618 9223 9868
shane@altocapital.com.au

Alan Lawson
Director
Phone: +618 9223 9878
alan@altocapital.com.au

Peter Hayes
Investment Manager
Phone: +618 9223 9836
peterh@altocapital.com.au

Stockley Davis
Corporate Manager
Phone: +618 9223 9835
stockley@altocapital.com.au

Cameron Bolton
Investment Manager
Phone: +618 9223 9832
cameron@altocapital.com.au

Chris McGrath
Investment Manager
Phone: +618 9223 9822
chris@altocapital.com.au

David Parker
Investment Manager
Phone: +618 9223 9830
david@altocapital.com.au

Ian Leete
Authorised Representative
Phone: 0415 707 065
ian@altocapital.com.au

Mathew Walker
Authorised Representative
Phone: +618 6460 4960
mathew@cicerocorporate.com.au

James Robinson
Authorised Representative
Phone: +618 6460 4960
james@cicerocorporate.com.au

Carey Smith
Research Analyst
Phone: +618 9223 9838
carey@altocapital.com.au

Andrea McIntosh
Administration Manager
Phone: +618 9223 9887
Andrea@altocapital.com.au

## Research Disclaimer/Disclosure

### Important Information

1. **Disclosure**:
   The author of this publication, Alto Capital, its Directors, Advisers, Associates and Employees from time to time may hold shares in the securities mentioned in this Research document and therefore may benefit from any increase in the price of those

securities. Alto Capital and its Advisers may earn brokerage, fees, commissions, other benefits or advantages as result of a transaction arising from any advice mentioned in publications to clients. Detailed disclosures are made below if applicable.

Some information within this document has been provided by Nemex Resources Ltd and Wavefront Biometric Technologies Pty Ltd.
Alto Capital and their associates hold shares in Nemex Resources Ltd.

2. **Disclosure of Interest:**
Alto Capital, its Directors, Advisers, Associates and Employees **at the time of releasing this report have the following interest in the shares mentioned in this research report:**
Leete Family Super Account owns 2665 shares in private company WBT (which were paid for circa $15,000)
Dashian Family Trust owns 750T shares left and 5M options (5 cents) which it paid 2 cents per share for.