SOUNDVIEW RESEARCH

NXT-ID INC. (OTC QB: TICKER $4.25)

MOBILE SECURITY BEYOND THE PASSWORD

STEPHEN WAITE AND KRIS TUTTLE – OCTOBER 15, 2013

INTRODUCTION

Table of Contents

There is a paradigm shift underway in the digital economy – one that has the potential to fundamentally change the way consumers, businesses and government agencies use and interact with technology. At the heart of the paradigm shift is a transition in payments processes and security technology away from conventional forms toward more advanced hardware and software. Device-level sensors, biometrics and embedded processing have arrived.

With these advanced technologies, the wallet can be made more versatile, secure and powerful with modern technology built into it. This same approach will be found in a broad range of products from firearms to autos, which will only fire and run if the authorized owner is securely identified and in command. The IT companies have provided more security (multi-factor, out-of-band authentication) but these don't work well because they are neither simple nor obvious. It's now pretty easy to know that "you are you" given enough of the right sensor and biometric information combined with the right data and some local processing.

In the future, it is likely that we are not going to carry around little pieces of colored plastic to make payments; furthermore, we are not going to rely on simple alphanumeric passwords to access our devices and conduct transactions. Lest everyone think the smartphone will save the day, it has a few chronic weaknesses. Power is the most basic one. Consumers expect their keys and wallet to work all the time. Smartphones are not secure or private in the slightest, nor are they likely to become so for quite some time.

The shifting digital economy landscape opens up new opportunities for entrepreneurs and investors alike. NXT-ID is an emerging technology company that is building an innovative, next generation platform using advanced biometric technology to enable secure transactions, identity management, and access control in an intuitive, cost-effective and easy-to-use manner. The company recently completed a public offering, and the shares are now publicly traded. The capital will be used to continue the development of their biometric security products.

NXT-ID's Mobile-Bio technology platform is the foundation for three new product offerings designed primarily to mitigate security risk of mobile devices. These products include a modular facial recognition system called Mobile-Bio FaceMatch,™ a separate, physical biometric secured electronic wallet called The Wocket,™ as well as a portable biometric device called Mobile-Bio Sensor,™ which allows an individual access through multiple devices to a protected database or server.

This segment has been active in terms of acquisitions. The first generation biometric security company (L-1 Identity Solutions) was acquired by security giant Safran for $1.6B in 2010. L-1 was predominantly enterprise focused and didn't address mobile or online commerce. Apple bought mobile security firm AuthenTec for a reported $356M, predominantly for their fingerprint sensor technology.

Our initial IV case suggests a stock value of $10.90/share if the company can execute on their plans.

THE OPPORTUNITY

The convergence of mobile and security technology is creating a host of new investment opportunities. Convergence is currently being driven by several factors. One key factor is the soaring functionality of mobile devices. This rising functionality is associated with the proliferation of smartphones in the market, which today exceed one billion users worldwide and counting.

Today's smartphones allow people to use their mobile devices in a variety of ways that extend far beyond making calls and texting, including banking, shopping, social media, playing music, taking pictures, and recording video, among many other things. In short, mobile commerce (m-commerce, for short) is growing today, with nearly one-third of mobile users having made a purchase with their phones.

The rising functionality of mobile devices and m-commerce is generating a greater demand for security that extends beyond conventional technology. Security has always been an important issue over the Internet and on the web. However, the dynamics are shifting amid an ever-rising incidence of online breaches.

"Passwords have failed. It's time to try something new."

-Mat Honan, Senior Writer, WIRED

The media headlines are rife with high profile hackings, some which are breath-taking in their scope and ingenuity. Consumers, corporations and government agencies have all been targets of hackers. It would appear that nobody is immune from security breaches. The costs associated with these incidents are anybody's guess; all we can say with confidence is that they are high and rising over time.

The disruptions associated with hacking can be monumental, as noted by WIRED senior writer, Mat Honan, in a high profile cover story for the magazine last year. Mat experienced a nightmare during the summer of 2012: his online identity was hacked. In the span of less than an hour, Honan felt as if his life was ruined. The hackers took his files, email and photos. [1] Following his nightmare, Honan soberly concluded a reality about the online world that is not well appreciated today by many: No matter how complex, no matter how unique, your passwords can no longer protect you.

[1] For more on Honan's experience see, "Kill the Password: Why a String of Characters Can't Protect Us Anymore," WIRED, December 2012.

We could not agree more with Mr. Honan. We have done a good deal of research in the information security segment over the years. It is clear to us that we are entering a period where there will be growing demand for security solutions that extend beyond the password and conventional token-based technologies. Combine the rising volume of transactions occurring over mobile devices today with the lack of online security and you have a recipe for opportunity and wealth creation in the months and years ahead.

Our research informs us there is a large opportunity for emerging technology companies in the market for biometric secure access control as consumers, enterprise, and government agencies around the world seek greater security. Biometric technology has the potential to meet that demand. NXT-ID was incorporated early last year with a mission to develop innovative, next generation biometric technology for secure access control. Below, we take a closer look at the company, its technology, market opportunity, competition/industry structure, and we assess its intrinsic value.

Company Overview

NXT-ID is an emerging technology company that is building an innovative, next generation information security platform using advanced biometric technology to enable secure transactions, identity management, and access control via mobile and other devices in an intuitive, cost-effective and easy-to-use manner. Led by CEO Gino Pereira and CTO David Tunnell, the company has three distinct lines of business: law enforcement, m-commerce, and biometric access control application.

NXT-ID recently completed a public offering and listed on the OTC QB. The capital will be used to launch several biometrics security products.

> *"NXT-ID is creating a new paradigm for information security beyond the password that is based on innovative biometric technology."*

NXT-IDs founders have experience managing emerging technology companies and running publicly traded companies. CEO Gino Pereira has over 30 years of executive, operational and financial experience with technology companies in the United States, Europe and the Far East. CTO David Tunnell is an expert in biometrics and is the inventor of a variety of miniature technologies for remote distributed sensors, with over two decades of experience in developing high-technology solutions for the U.S. government. He leads the company's talented and experienced software team, which is based in Florida.

NXT-ID's Board of Directors includes Major General David R. Gust, USA, Ret. General Gust retired from the United States Army in 2000 after completing a career of 34 years of service. His General Officer assignments included the Program Executive Officer, Communications Systems (PEO-Comm Systems), Program Executive Officer, Intelligence, Electronic Warfare and Sensors (PEO-IEW&S) and at Army Materiel Command, as Deputy Chief of Staff for Research, Development and Acquisition (DCSRDA).

NXT-ID is creating a new paradigm in information security. At the heart of the new paradigm is real-time, dynamic, multi-factor biometric authorization that is user friendly and extremely difficult to hack, thus providing greater security beyond conventional security systems. This system combines multiple attributes that are unique to each user (e.g., face, voice, fingerprint, retina) with multiple attributes that are unique to other identifiable features, such as devices and accounts, to form an impenetrable security solution.

This solution uses a real-time engine and dynamic security process for each login session or transaction so that the user experience is actually enhanced, versus the conventional static experience of typing in the same password. Introducing this new paradigm, NXT-ID hopes to shatter the conventional User/Password structure that currently exists by developing what they are appropriately calling "The un-Password" – where information security begins to rival Fort Knox, whether at home, on the road, or at the office.

NXT-ID's expertise in biometrics, along with its growing patent portfolio of cutting edge technology, gives the company a solid foundation upon which to make the new security paradigm a reality in the marketplace. The product roadmap is ambitious with several new security products scheduled for release in the months ahead, all of which leverage the company's Mobile-Bio™ platform. NXT-ID is using its Mobile-Bio platform to commercialize a range of next generation security products targeted at a range of applications. These products include:

1. **Mobile-Bio FaceMatch**™ – 2D, 3D and pseudo-3D methods to perform facial recognition. Additionally, NXT-ID seeking to incorporate its patent pending "FacePassword" as a method to add multi-factor face and face movement to Dynamic Pairing Codes using a simple low-power embedded processor on an external device (biosensor), such as a Wocket, that then connects to other end-points using Dynamic Pairing Codes. The non-Mobile version of FaceMatch is currently on the market and being used by various law enforcement agencies to provide identity authentication.

2. **The Wocket™** – a new class of biometrically secure mobile devices designed to replace the traditional wallet.

3. **Mobile-Bio Sensor**™ **–** a simple, web-enabled, biometric-enabled external device that is used for local authentication and remote authentication with the BioCloud and/or remote servers.

4. **VoiceMatch**™ – a unique biometric-enabled method to add multi-factor biometric identifiers (both speech and speaker recognition) to Dynamic Pairing Codes using a simple low-power embedded processor on an external device (e.g., BioSensor), such as a Wocket, that then connects to other end-points using NXT-ID's Dynamic Pairing Codes.

5. **Mobile** BioCloud™ – a cloud-based end-point (authentication service) to authenticate any "end-point" along a communication path, including external biosensors such as the Wocket and/or other PCs or servers along the path. A dynamic pairing code is sent to the BioCloud where it is combined with other "identifiers" (e.g., device serial number, master key, wallet key, dynamic pairing keys, Firmware key) dynamically (per NXT-ID's proprietary algorithm that selects which identifiers are used when) to issue a response, which is then compared by each end-point.

NXT-ID's Mobile-Bio platform is diverse and contains a host of proprietary, next generation security technologies. The diversity of the platform is a key asset. It reflects the experience and depth of the company's management and software developers in biometric technology. The platform that enables NXT-ID is able to produce a range of innovative products incorporating proprietary methods targeted at different applications and market segments.

The Mobile-Bio FaceMatch product is a core product offering in development that is currently in beta testing with several law enforcement agencies. FaceMatch provides a modular facial recognition system for smartphones, tablets, laptops and desktop computers. Access to devices via FaceMatch is dependent on the level of security desired by users, as well as the number of cameras available. NXT-ID is developing the software so it can be hosted on the device or through the cloud. The company is planning on creating FaceMatch apps for both the iPhone and Android platforms and will not retain any personal information of the user.

Later this year, NXT-ID will be launching The Wocket, representing its first new product launching off the Mobile-Bio platform. The Wocket is a separate physical electronic wallet that configures a single programmable card for credit cards, retail store cards, ID cards etc. The product is not intended to compete with smartphone wallets, which are emerging in the market today, but instead is targeted at a niche market of individual and business users who may not own a smartphone or are seeking a higher level of security for mobile transactions in a standalone device. The company plans on offering an insurance plan at a nominal cost to users who may desire additional protection in case their Wocket is misplaced or stolen. NXT-ID plans to partner with companies, including wallet manufacturers, to produce a range of Wocket products that appeal to different consumer tastes.

Following the commercial launch of the Wocket, NXT-ID intends to release its BioSensor product. The BioSensor is a portable biometric device that allows an individual access through multiple devices to a protected database or server. The product integrates some of the same technology as the Wocket, including Dynamic Pairing Codes and VoiceMatch. The BioSensor will be able to communicate with the intended device directly or remotely. Verification is through cloud-based identity management and information "BioCloud" assurance services that will be hosted by NXT-ID. This device will help to secure one aspect of the "BYOD" (Bring Your Own Device) computing trend, which is a growing concern among corporations today given that more and more employees are using their personal smartphones and tablets to connect to enterprise IT servers.

NXT-ID's Mobile BioCloud is integral to the new security paradigm and this service will be developed incrementally along with the company's other new products. The BioCloud is a cloud-based identification and authentication management system that works in conjunction with NXT-ID's biometric security products. For enterprise, the BioCloud will offer companies a way to integrate employee devices into the network while providing high-level security. BYOD (Bring Your Own Device) is a big issue in the enterprise today with a majority of companies now allowing employees to bring and use their own devices at work. NXT-ID's BioCloud service could help IT departments address the BYOD issue that is causing security-related headaches in many companies.

There are numerous other related products that can be developed from NXT-ID's Mobile-Bio platform in the future. These may include more advanced biometric devices that are passive and conform to wearable computing and products incorporating User Defined Sequences and Dynamic User Defined Sequences that would enhance security well beyond the password. We are at an early stage of the paradigm shift underway in the digital economy, as mentioned earlier. There is a scope for a great deal of innovation and new product commercialization in the years ahead.

Taken together, NXT-ID biometric security products target a broad market opportunity space that includes m-commerce, enterprise, law enforcement, defense and Homeland Security. A lot of research and development work has already been completed and related costs incurred, thus creating a favorable dynamic for commercialization in the months ahead. In the next two sections of the report, we take a closer look NXT-ID's biometrics security technology and assess the company's overall market opportunity.

TECHNOLOGY

The genesis of NXT-ID goes back to the days when the founders were an integral part of the senior management teams at Technest Holdings, Inc., and its subsidiary, Genex Technologies. Genex Technologies was launched in the mid-1990s to develop and commercialize the unique Rainbow® method of capturing 3D data. The Rainbow method utilizes structured light to capture 3D data.[2]

Genex has developed innovative technologies and products for all aspects of imaging, including capture, processing, display, and enhancement. The company's products range from 3D cameras to surveillance algorithms to integrated facial recognition systems. Genex and Technest have won awards from the U.S. Department of Defense, NIH, NIST and NSF, amounting to over $30 million in support of the technology. NXT-ID has licensed (exclusively in many markets) all the Technest /Genex technology. This technology is an important piece of the foundation upon which NXT-ID is developing its products.

Additionally, NXT-ID has also licensed, on a non-exclusive basis, distribution, manufacturing rights and know-how from Geometrix, Inc., a leading 3D imaging company using a different technical approach from Technest. This technology performed very favorably at the Face Recognition Vendor Test conducted by the National Institute of Science and Technology (NIST). NXT-ID also has key scientific and engineering personnel that have had key roles in the development of these technologies and have an important intellectual knowledge base that the company intends to leverage.

[2] Structured light is the process of projecting a known pattern of pixels (often grids or horizontal bars) onto a scene. The way that these deform when striking surfaces allows vision systems to calculate the depth and surface information of the objects in the scene. Structured light is used by a number of police forces for the purpose of photographing fingerprints in a 3D scene..

Biometrics Primer

Biometrics is used as a form of identification and access control. Biometric identifiers have long been used by government agencies and commercial enterprises to verify a person's identity. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals, andare based on physiological or behavioral characteristics. Physiological biometrics could be a human voice, fingerprint, DNA, face or body, while behavioral biometrics is associated with the behavior of a person. Physiological biometric identifiers are unique to individuals. This characteristic makes them attractive for use in verifying identity, both online and offline.

There are several factors that are used to assess the suitability and reliability of any traits used in biometric authentication. Among these factors are:

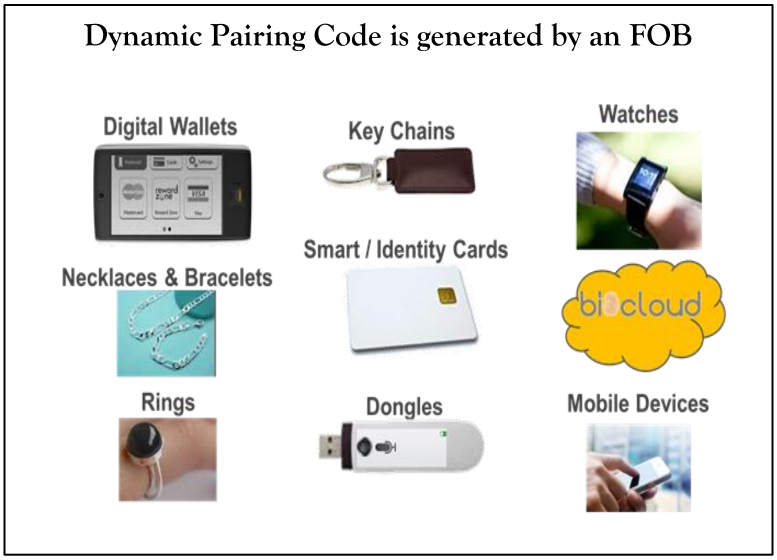
- **Universality**: Every person using a system should possess the trait (e.g. fingerprint, voice).
- **Uniqueness:** The trait should be sufficiently different for individuals in the relevant population such that they can be distinguished from one another.
- **Permanence:** Relates to the manner in which a trait varies over time; a trait with good permanence will be reasonably invariant over time with respect to the specific matching algorithm.
- **Measurability** (collectability): Relates to the ease of acquisition or measurement of the trait.
- **Performance:** Relates to the accuracy, speed, and robustness of technology used. **Acceptability:** Relates to how well individuals in the relevant population accept the technology such that they are willing to have their biometric trait captured and assessed.
- **Circumvention:** Relates to the ease with which a trait might be imitated using an artifact or substitute.

Biometric technologies can be evaluated based on these factors to assess their overall efficacy for use in authentication. While there is no single biometric that meets all the requirements of every possible application, there are several that can be used today to provide security online that exceeds passwords and tokens.

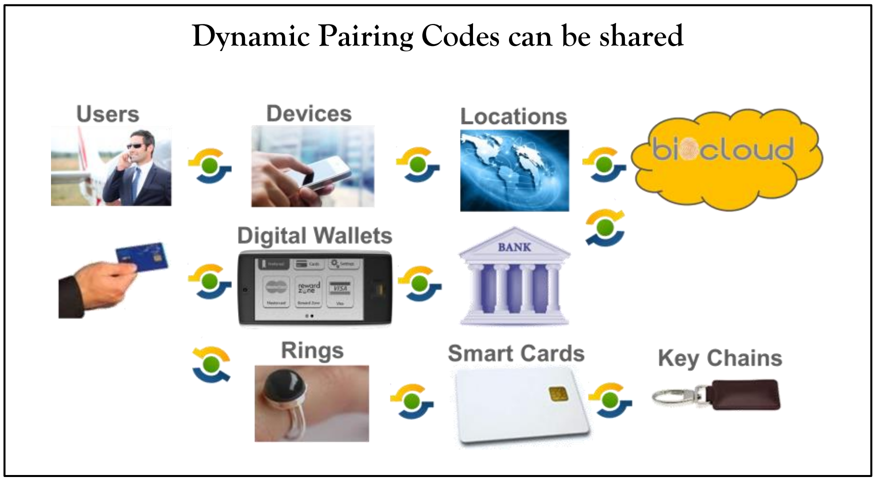
NXT-ID's technology also includes the acquired assets of 3D-ID, LLC, which is comprised of 22 licensed patents in the field of 3D facial recognition. NXT-ID is in the process of building out its extensive IP portfolio further by vigorously pursuing new patents associated with its new Mobile-Bio technologies, which includes The Wocket, The Mobile-Bio Sensor and FaceMatch products.

Another technology in development that figures prominently in the evolution of NXT-ID's biometric security paradigm is Dynamic Pairing Codes (DPC). DPC are a new, proprietary method to secure users, devices, accounts, locations and servers over any communication media by sharing key identifiers, including biometric-enabled identifiers, between end-points by passing dynamic pairing codes (random numbers) between end-points to establish sessions and/or transactions without exposing identifiers or keys.

Under Dynamic Pairing, any two or more entities can share specific information, or ***identifiers***, between themselves in order to establish recognition for a one time communication session or transaction. These identifiers and keys are unique to specific factors that include but are not limited to users, manufacturers, devices, accounts, locations and/or sessions (or transactions). Internal keys are derived from the identifiers so that all points have common information that "binds" or "pairs" the devices together (so that they have a means to recognize one another).


Dynamic Pairing Code is generated by an FOB

The way Dynamic Pairing works is for an entity to pass a randomly generated number to all the other entities to be "paired" together (see figure below). Authentication is performed when one entity passes a random code to another entity, which thereby sends a second pseudo-random number back to the first. The second pseudo-random number response is derived by generating a new pseudo-random number from a combination of the received random number and internal identifiers.


Dynamic Pairing Codes can be shared

The combination of which identifiers are used to generate the Dynamic Pairing Code is also dynamic, chosen by every point in the communication by NXT-IDs proprietary algorithm. Other inputs may also be used for key generation including a random number generator, temporary keys, and data from external sources to further customize the internal Dynamic Pairing Codes.

MARKET OPPORTUNITY

The market opportunity for NXT-ID's biometric security products is significant. The Wocket has a target market of nearly $1B in the U.S. alone. The opportunity will expand across multiple segments, given that the company's products target consumers, enterprise and government agencies in the U.S. and overseas. We can assess the overall opportunity for NXT-ID by analyzing the market for each its of three products.

NXT-ID's Wocket product is the next generation of secure wallets designed to function anywhere credit cards are accepted. There are close to 200 million credit card holders in the U.S. alone and tens of millions more overseas. The average credit card holder today has 3.5 cards. Credit cards are associated with more than $2.5 trillion in transactions a year and are accepted at more than 24 million locations in more than 200 countries and territories.

Fraud is a key concern of credit card users. There is growing demand for solutions that prevent or substantially curtail the incidence of credit card fraud. The Wocket has been designed to offer consumers an affordable, mobile, biometrically secured device that has security features and functionality exceeding anything on the marketplace today. In addition, NXT-ID is planning on offering users an inexpensive monthly insurance plan for frequent credit card users that seek even greater peace of mind.

NXT-ID strategy is to partner with banks and other financial services companies and make The Wocket available in the U.S. and, eventually, overseas. The company has also discussed the potential of partnering with EZ Pass, which are popular devices that ease traffic congestions on toll roads and speed along travel. EZ Pass transponders are in an estimated 22 million vehicles today, accounting for 2.5 billion transactions annually. The Wocket will also be designed to carry grocery cards, gas cards and other retail store cards that have become widespread, thus expanding its functionality to users beyond credit cards.

The Wocket is being designed to exploit Near Field Communications (NFC) technology as a way to transmit secure information over mobile devices. NFC is an emerging technology that has yet to take off, but there certainly seems to be a great deal of potential for the technology in the years ahead. We have seen analyst estimates of global, consumer financial sales transactions via NFC mobile-enabled devices growing to $50 billion by 2014. Total e-commerce sales worldwide today exceed $1 trillion, with an expected increase in market penetration of NFC-related mobile transactions in the future.

The Rise of NFC

Near field communication (NFC) is a set of standards for smartphones and other mobile devices to establish radio communication with each other by touching them together or bringing them into close proximity, usually no more than a few centimeters. Consumer electronics manufacturers Nokia, Philips and Sony founded the NFC Forum in 2004 to foster the development and standardization of NFC technology. The NFC Forum has more than 160 members today.

NFC technology facilitates the wireless exchange of information/content and has built-in capabilities to support secure applications, thus making it useful for payments applications and access control. NFC technology evolved from a combination of contactless identification (RFID) and interconnection technologies. There are security issues associated with NFC that may impede the rate of adoption of the technology in the m-Wallet segment.

We estimate that NXT-ID can capture 6 million users in the U.S. for its Wocket product. Based on the estimated selling price of The Wocket at $99.99 per unit, and including the optional insurance program and other ancillary services we peg the U.S. market opportunity for NXT-ID'S Wocket is estimated to be in the range of $780M to $930M.

The two other NXT-ID products scheduled for commercial launch – Mobile-Bio FaceMatch and Mobile-Bio Sensor – expand the company's overall market opportunity significantly beyond The Wocket.

With respect to the company's FaceMatch product, we note that facial recognition technology is emerging today among competing biometric technologies as one that is reliable and socially acceptable. The reliability factor is important in terms of use for access control and law enforcement. Social acceptance is a key issue for individuals as many people find some forms of biometrics intrusive (e.g. a retina scan).

> *"Thick skin will be a necessity for technology companies in the coming years of the digital age, because they will find themselves beset by public concerns over privacy, security and user protections."*
>
> -Eric Schmidt, Executive Chairman, Google

The market for facial recognition security technology exceeds $1 billion today, and is projected to grow at a 30%-plus clip in the years ahead. 3-D facial recognition technology – an area of core expertise for NXT-ID – is gaining wider use for access control by organizations. 3-D technology is well suited for identity verification. 3-D face readers can be used in conjunction with PINs, access control cards and other biometrics for multifactor authentications. In terms of speed and accuracy, 3D face recognition is as fast and accurate as fingerprint technology.

Facial recognition technology is not widely used as a way to access mobile devices today, but that is likely to change in the years ahead. The use of biometrics with mobile devices, such as smartphones, has the potential to grow rapidly in coming years with new applications such as NXT-ID's FaceMatch. NXT-ID envisions its FaceMatch product as becoming a popular app available for smartphone platforms such as Apple's iTunes and Google's Android. Mobile device users would undoubtedly respond favorably to an app that creates a secure access control environment, helps prevents fraud, is easy to use, and attractively priced.

Facial recognition security technology could become an important driver of m-commerce in the years ahead. The m-commerce ecosystem continues to develop and expand around the world, with many key players announcing plans for mobile payments, including AT&T, Sprint, Verizon, T- Mobile, Google, Visa, MasterCard, American Express, Discover, Bank of America, Barclays, and others.

The projected future growth of payments via mobile devices, which today is around $250 billion worldwide and projected by some analysts to rise to over $1 trillion over the next five years, is highly dependent on how consumers perceive the security of such devices for conducting financial transactions. Fraud is at the top of consumer concerns about using mobile devices for transactions. Biometric technology on mobile devices has the potential to play a key role in fostering security and preventing fraud while facilitating growth of m-commerce. NXT-ID plans to seek the support and sponsorship of credit card companies, financial institutions, and smartphone vendors who are seeking to offer customers greater security and fraud protection.

Outside of mobile devices, there is ample opportunity for growth of advanced facial recognition technology in law enforcement and defense. A tragedy in Florida involving a mistakenly identified prison inmate and police deputy hits home.[3] There is also a rapidly growing trend of ID fraud whereby criminals are filing bogus tax forms to claim refunds and exploiting a slow-moving federal bureaucracy. According to the U.S. Treasury Department, such activity could cost the nation tens of billions of dollars.

These types of events and activities are costly and need to be addressed in a timely and effective manner. NXT-ID's technology is working closely today with several established system integration firms today including Battelle Memorial Institute, Verizon Federal Systems and EOIR Technologies (a prime contractor with the Night Vision Electronic Sensors Directorate).

NXT-ID's Mobile-Bio Sensor product enlarges the company's market opportunity by targeting the rapidly growing BYOD phenomenon in the enterprise space. As mentioned earlier, BYOD has become a significant issue in the enterprise today with a majority of companies now allowing employees to bring and use their own devices at work.

As physical security converges with IT security, we will likely see the use of smartphones as access control devices (as opposed to physical cards or punching in numbers on a key pad). This will only serve to heighten the need for additional security over mobile devices and to drive demand for products such as NXT-ID's Fingerprint Sensor.

There is a significant market opportunity for NXT-ID with its suite of Mobile-Bio biometric security products. This opportunity is reflected in the financial modeling and valuation work discussed below. Before presenting that analysis, we will take a look at the company's competitive landscape and industry dynamics.

Competition and Industry Dynamics

NXT-ID's Mobile-Bio suite of biometric solutions is designed to enhance mobile security and provide next generation security for law enforcement and defense applications. The company's suite of security products offers distinct advantages in the marketplace. NXT-ID sees a role for products that fill an interoperability gap left by traditional biometric solutions. Many competing products on the market today are physically integrated and thus not flexible or versatile for widespread use in the mobile segment. NXT-ID plans to develop and foster market niches targeted at consumers and small business while continuing to serve the law enforcement and defense markets.

**Mobile Wallets:
Coming of Age**

NXT-ID Wocket
Google Wallet
V.me (Visa, MasterCard)
PayPass Wallet
ISIS
Square Wallet
iCache
Lemon Wallet
LevelUp,
PayPal

Given the problems associated with conventional security solutions today, we expect to see a proliferation of new biometrics products coming to the market in the future. Competition is likely to intensify in NXT-ID's core markets, especially in the emerging mobile wal-

[3] For more on this tragic story, see FlordiaToday.com: http://www.floridatoday.com/article/20130207/NEWS01/302070041/.

let segment. Many of the company's primary competitors are well-established corporations that have substantially greater financial, managerial, technical, marketing, personnel and other resources than it does today. Google and Apple, for example, are both developing facial recognition applications for their respective Android and iOS mobile platforms.

Google is also moving aggressively in the m-commerce segment with its Android mobile application "Google Wallet." Google has partnered with Citibank, Mastercard, First Data, VeriFone, Samsung and Sprint and other companies to create an ecosystem supporting its Wallet application. Visa and Mastercard have their own m-Wallet venture called "V.me." Another competing ecosystem includes communications giants AT&T, T-Mobile, and Verizon, who have partnered to create a virtual wallet and payment system called "ISIS." ISIS is an open platform that extends to all merchants, banks and carriers. The application eliminates the need to carry cash, credit cards and debit cards, reward cards, coupons, tickets and transit passes.

With ISIS, the smartphone becomes a wallet. The ISIS app is PIN protected. Personal data is stored on a special chip in the users phone. If a phone is lost or stolen, users can call or go online to freeze payment of cards loaded onto the application, just as one would do if a physical card were lost or stolen. If the phone is recovered, the application can be activated in a similar manner.

Another emerging player is Square, a company backed and led by Twitter co-founder Jack Dorsey. Square has device that plugs into smartphones that enables mobile transactions. The company is currently processing payments at a $5 billion annualized rate. Other companies vying for penetration in the m-Wallet segment are PayPal, PayPass Wallet, Lemon Wallet and LevelUp.

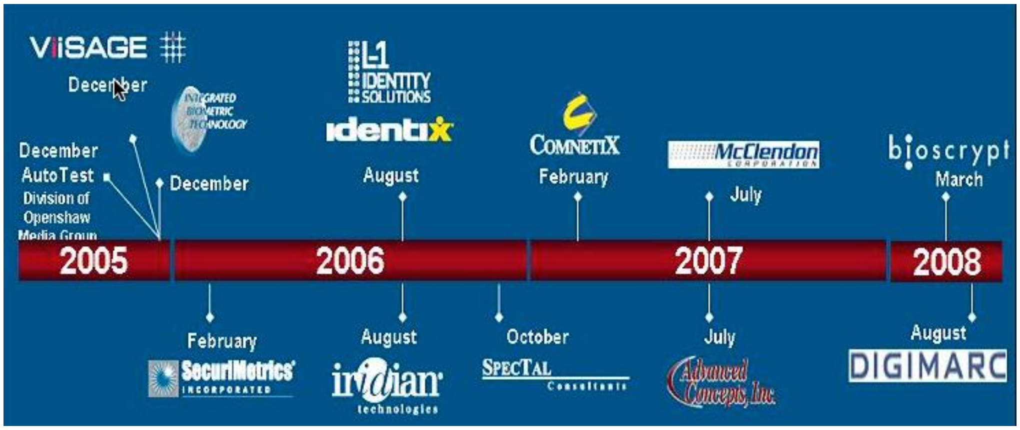
Based on various surveys we have seen, there is likely to be growing acceptance of the m-Wallet technology in the months and years ahead. That said, security will be a key element driving market adoption. It is incumbent upon companies to offer customers secure mobile transaction capability as well as ease of use and convenience. At this juncture, the market for m-Wallets is wide open and NXT-ID will have an opportunity for vie for a share as the company ramps up.

Outside of the m-Wallet segment, there are numerous independent suppliers of biometric products in the market competing against NXT-ID. One of the largest today is L1 Identity Solutions. L1 is a vertically integrated biometric solutions provider with a large established base of business. The company has well established marketing channels with government agencies. Another established supplier is Cognitec, a German-based facial recognition company with worldwide distribution capabilities.

Related Transactions

From 2005 to 2008 there was a big roll-up of biometric security technologies and companies which culminated in one company, L-1 Identity Solutions, owning the whole lot of them. As the figure below shows, the prodigious series of acquisitions included 3D facial recognition, fingerprint technology, iris recognition, secure documents and a range of supporting services and IP around those areas. In September of 2010 L-1 Identity Solutions was acquired by security market giant Safran for $1.6 billion. The unit now does business under the MorphoTrust USA brand.

In July of 2012 Apple bought mobile security firm AuthenTec for a reported $356M mostly for their fingerprint sensor technology. This fact is fairly clear from filing documents of the transaction and further supported by the fact that they subsequently divested the AuthenTec embedded security business to Inside Secure (EPA: INSD) for $48M.



At the end of 2010 ASSA ABLOY acquired biometric card maker LaserCard for $80M (a 42% premium to their public market price at the time.) At the time of the acquisition LaserCard was earning about $3.5M on $50M in sales. This puts the transaction value at 22x operating earnings and 1.6x sales. In the years leading up to the deal LaserCard had a spotty record of growth with intermittent profitability.

Although this list of related transactions is not exhaustive it's illustrative of the strategic value ascribed to mobile security and biometrics. Even in cases where management teams haven't been able to deliver consistent growth and margin expansion they have created asset value that rarely goes wanting in the M&A marketplace.

INTRINSIC VALUATION

Valuation is always tricky for emerging technology companies. However, we can still apply our IV methodology to these situations if we first derive our revenue model from known market size and dynamics, future adoption rates and market share. The background behind our model is below but in summary our base case IV estimate is $10.90 for 2014. The model itself is included as an appendix.

NXT-ID is targeting more than one market but for the purposes of our IV model we are going to exclude business from FaceMatch and biometric applications like BioSensor and BioCloud. If these other product areas become material we will incorporate them into our forecast.

During the next few years NXT-ID revenues will be dominated by the Wocket e-wallet solution and supplemental insurance, which is a high-margin add-on. The most relevant potential market for the Wocket is initially the US credit card consumer, which totals about 200m individuals. There are approximately 1B credit cards in circulation based on figures provided by American Express, MasterCard and Visa.

There are some demonstrated metrics around the adoption of new services so we can use those to estimate how large the ultimate market will be. The opening rule of thumb is the "30/10/10" rule, which means that 30% of the target user base will download and try the service, 10% of those will become regular users and 10% of those will be "power" users who use the product or service multiple times a day.

Using our basic math we can expect 60M users to try an e-wallet service if they were all made aware of it and given an opportunity try it. Of those, 6M would become active paying users and nearly one million of those would become intense users who would be included to buy additional related services. Our model assumes a $99 price point for an initial target market size of $530M on the purchase side of the business with an additional 15% per year for supplemental services, maintenance and support. The high end user category is worth an additional $150M plus a similar 15%. All together this provides an initial market opportunity of $680M plus another $100M to $250M in ancillary service and maintenance fees.

The next two questions are 1) how fast will people adopt the e-wallet, and 2) what share of this e-wallet market will NXT-ID get. For us these two are actually tied together because the nature of the NXT-ID solution has a direct impact on adoption. Convenience and reliability are two of the hallmarks of what enables a new service to take root with consumers. The Wocket has the advantage of working with the existing credit/debit card infrastructure and not requiring a smartphone for support.

On the consumer side, one of the best proxies for adoption rate at the individual consumer level is LifeLock (NYSE: LOCK), which provides consumer identity and fraud protection. LifeLock has over 2.3M members but has built that base over time by adding 200,000 or so (net) members per year. The ramp at LifeLock has been much steadier so far than one might expect. The customer acquisition period really started 10 years ago in 2002. The 200,000 annual added membership figure is no inflection point. That said, LifeLock spent $123M in 2012.

We've put a stake in the ground on Wocket sales as shown in our model. We've based our initial figures on resources the company will have post-offering and further assume that one significant partner is added in 2014. Assuming that the product ships on time and meets expectations, the first year sales are a function of market reach. Initially, the company has limited resources to dedicate to marketing but early sales will go a long way to help attract much larger partners. If the company adds additional partners then our numbers would be revised upward. Key figures in the near-term are sales of 150,000 units in 2013 and 600,000 units in 2014.

CONCLUSION

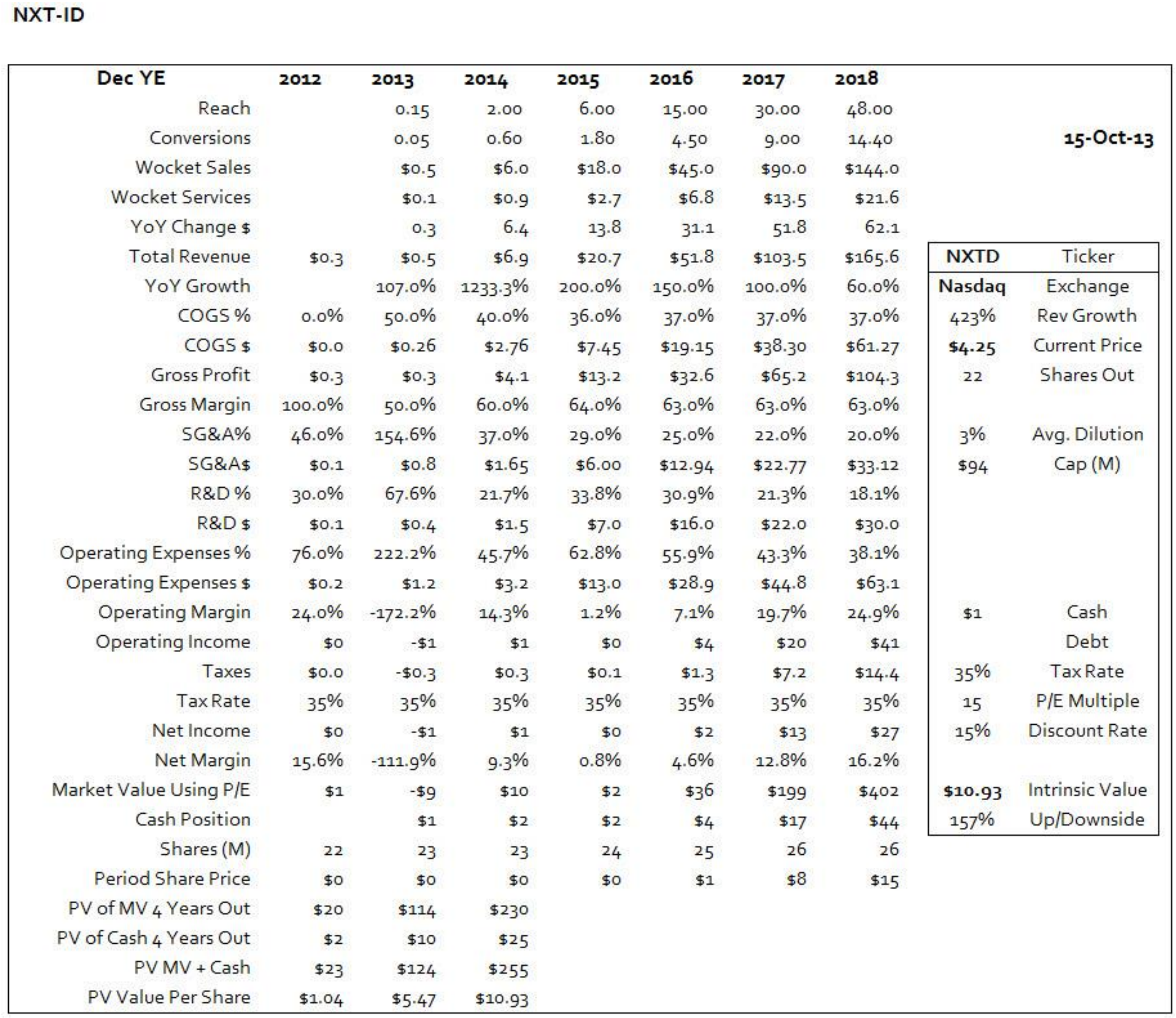
Like many technologists our reflex on mobile payments is to jump to the conclusion that the smartphone is the answer. Now we know that it isn't, not now and not for years. Consumers love mobile devices but they are acutely aware and deathly afraid of intrusions that compromise their data, privacy and – most of all – their money. Investors should also consider the fact that smartphones have major hard-to-solve power issues and most of the payment infrastructure in the world will be looking for a credit card or "virtual credit card" like those produced by the NXT-ID Wocket.

As an emerging company we are well aware of the long and arduous road that NXT-ID and their investors must follow. However, they have a superior vision into this segment of the market and a meaningful base of IP and late-stage product development to use in driving revenue and earnings.

The next year will be a careful building year for NXT-ID and their investors. Our IV makes it clear that there is tremendous upside for investors if the company comes close to delivering on their plans.

Themes like mobile, security and commerce are coming together and becoming top-of-mind for many investors, and this should help NXT-ID gain attention from investors as they grow.

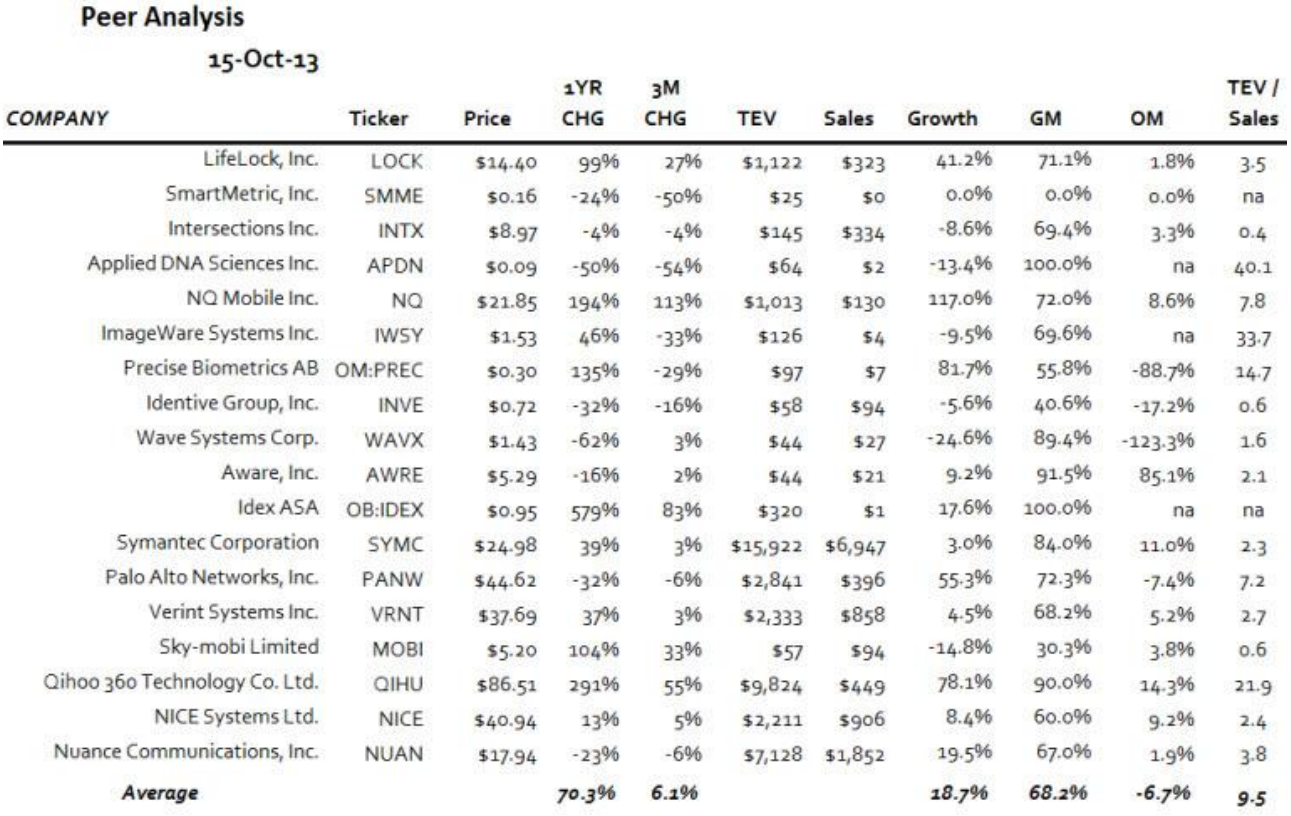
APPENDIX: INTRINSIC VALUATION MODEL



NXT-ID

Dec YE	2012	2013	2014	2015	2016	2017	2018		
Reach		0.15	2.00	6.00	15.00	30.00	48.00		
Conversions		0.05	0.60	1.80	4.50	9.00	14.40		**15-Oct-13**
Wocket Sales		$0.5	$6.0	$18.0	$45.0	$90.0	$144.0		
Wocket Services		$0.1	$0.9	$2.7	$6.8	$13.5	$21.6		
YoY Change $		0.3	6.4	13.8	31.1	51.8	62.1		
Total Revenue	$0.3	$0.5	$6.9	$20.7	$51.8	$103.5	$165.6	**NXTD**	Ticker
YoY Growth		107.0%	1233.3%	200.0%	150.0%	100.0%	60.0%	**Nasdaq**	Exchange
COGS %	0.0%	50.0%	40.0%	36.0%	37.0%	37.0%	37.0%	423%	Rev Growth
COGS $	$0.0	$0.26	$2.76	$7.45	$19.15	$38.30	$61.27	**$4.25**	Current Price
Gross Profit	$0.3	$0.3	$4.1	$13.2	$32.6	$65.2	$104.3	22	Shares Out
Gross Margin	100.0%	50.0%	60.0%	64.0%	63.0%	63.0%	63.0%		
SG&A%	46.0%	154.6%	37.0%	29.0%	25.0%	22.0%	20.0%	3%	Avg. Dilution
SG&A$	$0.1	$0.8	$1.65	$6.00	$12.94	$22.77	$33.12	$94	Cap (M)
R&D %	30.0%	67.6%	21.7%	33.8%	30.9%	21.3%	18.1%		
R&D $	$0.1	$0.4	$1.5	$7.0	$16.0	$22.0	$30.0		
Operating Expenses %	76.0%	222.2%	45.7%	62.8%	55.9%	43.3%	38.1%		
Operating Expenses $	$0.2	$1.2	$3.2	$13.0	$28.9	$44.8	$63.1		
Operating Margin	24.0%	-172.2%	14.3%	1.2%	7.1%	19.7%	24.9%	$1	Cash
Operating Income	$0	-$1	$1	$0	$4	$20	$41		Debt
Taxes	$0.0	-$0.3	$0.3	$0.1	$1.3	$7.2	$14.4	35%	Tax Rate
Tax Rate	35%	35%	35%	35%	35%	35%	35%	15	P/E Multiple
Net Income	$0	-$1	$1	$0	$2	$13	$27	15%	Discount Rate
Net Margin	15.6%	-111.9%	9.3%	0.8%	4.6%	12.8%	16.2%		
Market Value Using P/E	$1	-$9	$10	$2	$36	$199	$402	**$10.93**	Intrinsic Value
Cash Position		$1	$2	$2	$4	$17	$44	157%	Up/Downside
Shares (M)	22	23	23	24	25	26	26		
Period Share Price	$0	$0	$0	$0	$1	$8	$15		
PV of MV 4 Years Out	$20	$114	$230						
PV of Cash 4 Years Out	$2	$10	$25						
PV MV + Cash	$23	$124	$255						
PV Value Per Share	$1.04	$5.47	$10.93						

APPENDIX: PEER GROUP OF RELATED COMPANIES



Peer Analysis

15-Oct-13

COMPANY	Ticker	Price	1YR CHG	3M CHG	TEV	Sales	Growth	GM	OM	TEV / Sales
LifeLock, Inc.	LOCK	$14.40	99%	27%	$1,122	$323	41.2%	71.1%	1.8%	3.5
SmartMetric, Inc.	SMME	$0.16	-24%	-50%	$25	$0	0.0%	0.0%	0.0%	na
Intersections Inc.	INTX	$8.97	-4%	-4%	$145	$334	-8.6%	69.4%	3.3%	0.4
Applied DNA Sciences Inc.	APDN	$0.09	-50%	-54%	$64	$2	-13.4%	100.0%	na	40.1
NQ Mobile Inc.	NQ	$21.85	194%	113%	$1,013	$130	117.0%	72.0%	8.6%	7.8
ImageWare Systems Inc.	IWSY	$1.53	46%	-33%	$126	$4	-9.5%	69.6%	na	33.7
Precise Biometrics AB	OM:PREC	$0.30	135%	-29%	$97	$7	81.7%	55.8%	-88.7%	14.7
Identive Group, Inc.	INVE	$0.72	-32%	-16%	$58	$94	-5.6%	40.6%	-17.2%	0.6
Wave Systems Corp.	WAVX	$1.43	-62%	3%	$44	$27	-24.6%	89.4%	-123.3%	1.6
Aware, Inc.	AWRE	$5.29	-16%	2%	$44	$21	9.2%	91.5%	85.1%	2.1
Idex ASA	OB:IDEX	$0.95	579%	83%	$320	$1	17.6%	100.0%	na	na
Symantec Corporation	SYMC	$24.98	39%	3%	$15,922	$6,947	3.0%	84.0%	11.0%	2.3
Palo Alto Networks, Inc.	PANW	$44.62	-32%	-6%	$2,841	$396	55.3%	72.3%	-7.4%	7.2
Verint Systems Inc.	VRNT	$37.69	37%	3%	$2,333	$858	4.5%	68.2%	5.2%	2.7
Sky-mobi Limited	MOBI	$5.20	104%	33%	$57	$94	-14.8%	30.3%	3.8%	0.6
Qihoo 360 Technology Co. Ltd.	QIHU	$86.51	291%	55%	$9,824	$449	78.1%	90.0%	14.3%	21.9
NICE Systems Ltd.	NICE	$40.94	13%	5%	$2,211	$906	8.4%	60.0%	9.2%	2.4
Nuance Communications, Inc.	NUAN	$17.94	-23%	-6%	$7,128	$1,852	19.5%	67.0%	1.9%	3.8
Average			***70.3%***	***6.1%***			***18.7%***	***68.2%***	***-6.7%***	***9.5***

COMPANY DESCRIPTIONS[4]

LifeLock, Inc. provides identity theft protection services for consumers; and identity risk assessment and fraud protection services for enterprises in the United States. It protects consumer subscribers through monitoring identity-related events, such as new account openings and credit-related applications; and enterprise customers through delivering on-demand identity risk and authentication information about consumers. The company offers LifeLock Identity Alert system, which provides its members with real-time alerts and a response system for identity threats through text message, phone call, or e-mail; and ID Score, an identity risk service that delivers on-demand assessment of the risk of an individual at account opening and throughout the customer lifecycle. As of June 30, 2012, the company served approximately 2.3 million paying members; and 250 enterprise customers, including financial institutions, telecommunication and cable services providers, government agencies, technology companies, large retailers, automobile and mortgage lenders, and e-commerce providers. LifeLock, Inc. was founded in 2005 and is headquartered in Tempe, Arizona.

SmartMetric, Inc., a development stage company, engages in the research and development of biometric security solutions. Its principal product includes Biometric Datacard, a fingerprint sensor activated card with a finger sensor onboard the card and a built-in fingerprint reader with a rechargeable battery for portable biometric identification. The company's Biometric Datacard has various security applications, such as employee identity, building access and security control, computer network access, driver's licenses,

[4] Descriptions sourced from S&P Capital IQ

passports, welfare payments, health insurance, portable electronic medical records, and check cashing identity verification, etc. SmartMetric, Inc. was founded in 2002 and is based in Las Vegas, Nevada.

Intersections Inc. provides subscription based consumer protection services and other consumer products and services primarily in the United States. The company operates in three segments: Consumer Products and Services, Online Brand Protection, and Bail Bonds Industry Solutions. The Consumer Products and Services segment offers identity theft protection and credit information management products and services, such as credit reports, credit monitoring, credit scores, credit education, reports and monitoring of additional information, identity theft recovery, identity theft cost reimbursement, and software and other technology tools and services. This segment also provides data breach response; accidental death and disability insurance; and other membership products and services, as well as access to healthcare, home, auto, financial, and other services and information. The Online Brand Protection segment offers online brand protection services comprising online channel monitoring, auction monitoring, and other services, as well as forum, blog, and newsgroup monitoring services to corporate brand owners or law firms. The Bail Bonds Industry Solutions segment provides automated service solutions for the bail bonds industry, which include accounting, reporting, and decision making tools that allow bail bondsmen, general agents, and sureties to run their offices, to exercise operational and financial control over their businesses, and to make underwriting decisions. The company was founded in 1996 and is headquartered in Chantilly, Virginia.

Applied DNA Sciences, Inc. provides botanical-DNA based security and authentication solutions in Europe and the United States. The company offers SigNature DNA markers for embedding into a range of products, including various inks, dyes, textile treatments, thermal ribbon, thread, varnishes, and adhesives; SmartDNA, a patented security system for stores, warehouses, banks, pharmacies, ATMs, and the protection of valuables; and DNANet tactical DNA products for law enforcement in the form of DNA-marked sprays and liquids. It also provides BioMaterial GenoTyping solution that develops genetic assays to distinguish between varieties or strains of biomaterials, such as cotton, wool, tobacco, fermented beverages, natural drugs, and foods, which contain their own source DNA; digitalDNA, a DNA-secured form of the quick read code to create customer interface; and Cashield, a range of cash degradation inks that permanently stain banknotes stolen from cash-handling or ATM systems. The company offers its products and solutions for use in the protection of products, brands, and intellectual property of companies, governments, and consumers from theft, counterfeiting, fraud, and diversion. The company was formerly known as Datalink Systems, Inc. and changed its name to Applied DNA Sciences, Inc. in 2002. The company was founded in 1983 and is headquartered in Stony Brook, New York.

NQ Mobile Inc. operates as a provider of mobile Internet services focusing on security, privacy, and productivity worldwide. Its cloud-client computing platform combines its cloud-side mobile security knowledge repository and client-side applications to provide real-time mobile anti-malware, anti-spam, privacy protection, data backup and restore, and other services. The company offers mobile security services, including mobile malware scanning, Internet firewall, account and communication safety, anti-theft, performance optimization, hostile software rating and reporting, and other services to protect users from mobile malware threats, data theft, and privacy intrusion; and mobile privacy services that allow users to store and modify contacts, call logs, SMS, videos, and pictures in a secure environment. It also provides mobile productivity services comprising screening incoming calls, filtering unwanted spam, SMS messages, protecting communication privacy, and managing calendar activities, as well as cloud-side synchronization of personal data, such as address books, text messages, calendars, and other data to enhance time and relationship management. In addition, NQ Mobile provides personalized cloud services that utilize synchronized user information to provide tailored user experience and extend the functionalities of its core services. Further, the company offers user-centric client-side mobile security, privacy, and productivity applications optimized for mobile devices. It offers Freemium subscription services to approximately

242 million registered user accounts in approximately 150 countries. The company was formerly known as NetQin Mobile Inc. and changed its name to NQ Mobile Inc. in April 2012. NQ Mobile Inc. was founded in 2005 and is headquartered in Beijing, the People's Republic of China.

ImageWare Systems Incorporated provides biometrically enabled software-based identity management solutions. The company offers IWS Biometric Engine, which enables the enrollment and management of population sizes; IWS PIV (personal identity verification) management application that supplies the Web-based graphical user interface to various server functions; IWS PIV Middleware product, which connects a card reader and PIV card; IWS Background Server, a software application designed for biometric identity management functions; IWS Desktop Security, a modular authentication management platform; and IWS Biometric Quality Assessment and Enhancement, a biometric image enhancement and assessment solution. It also provides IWS Card Management System to support and manage the issuance of smart cards; IWS EPI Suite, an ID software solution for producing, issuing, and managing credentials and personal identification cards; IWS EPI Builder, which offers various aspects of ID functionality; IWS EPI PrintFarm software for card printing; IWS PIV Encoder that programs the PIV smart cards; and IWS Law Enforcement, a digital booking, identification, and investigative solution. In addition, the company offers various software modules comprising Capture to capture and store images and text information; Livescan to capture prints and palm data; Investigative that creates a catalogue of possible matches; Facial Recognition to identify possible suspects and persons using multiple aliases; Law Enforcement (LE) Web that enables personnel to access and search agency booking records; and EPI Designer for Law Enforcement, a design solution. It primarily serves schools, universities, airports, hospitals, border crossings, corporations, and government agencies in the United States, Australia, Canada, the United Arab Emirates, Kuwait, Mexico, Colombia, Costa Rica, Venezuela, Singapore, Indonesia, and the Philippines. The company was founded in 1987 and is headquartered in San Diego, California.

Precise Biometrics AB (publ) provides biometric solutions to enterprises and government worldwide. Its solutions replace keys, PIN codes, and passwords; and enhances security during the use of ID cards and passports. The company operates in two segments, Mobile, and Identity and Authentication Management (IAM). The Mobile segment offers hardware, software, and services focusing on the mobile sector for smartphones and tables. This segment's solutions include Tactivo, a smart case for iPhone and iPad with embedded smartcard and fingerprint readers. The IAM segment offers a range of solutions, including embedded solutions for national ID cards, government agencies, banks, and companies. It offers fingerprint readers; Precise Match-on-Card technology that enables the matching and storage of fingerprints on smart cards; and Precise BioMatch Embedded, a solution for integration in various hardware devices for payment terminals, access control systems, and banking services. This segment also provides physical access solutions for use in various premises. In addition, the company offers systems integration, integration support, testing and evaluation, systems design, upgrading support, and training services. It markets its solutions and products directly and via a network of partners, including smart card manufacturers, systems integrators, resellers, and hardware and chip manufacturers to countries, government agencies, corporations, and organizations. Precise Biometrics AB (publ) was founded in 1997 and is headquartered in Lund, Sweden.

Identive Group, Inc. provides secure identification (ID) solutions that combine the convenience of radio frequency identification (RFID) with the security of smart card technology to enable people to interact with and manage digital devices, systems, and data. The company operates in two segments, Identity Management Solutions and Services, and Identification Products and Components. The Identity Management Solutions and Services segment designs, supplies, and manages solutions, systems, and services that enable the secure management of credentials. It provides integrated physical and logical access systems, integrated ID solutions, cashless payment solutions, and cloud-based credential management systems, designed to enable organizations provide convenience and speed for users while supporting security and compliance to regulatory requirements. This segment sells its solutions under the Hirsch Identive, idOnDemand, and Multicard brands to end customers that operate in the government, education, enterprise, and commercial markets; and in multiple vertical market segments, such as healthcare, banking, industrial, retail, and critical infrastructure. The Identification Products and Components segment designs and manufactures RFID and smart card technology-based products and components, including NFC products and components, that are used in the government, enterprise, and consumer markets for various identity-based and related applications, such as logical access, physical access, eHealth, eGovernment, citizen ID, mobile payments, loyalty schemes, and transportation and event ticketing primarily under the Identive brand. The company markets its products through OEMs, distributors, dealers, system integrators, value-added resellers, resellers, and Internet. The company was formerly known as SCM Microsystems, Inc. and changed its name to Identive Group, Inc. in June 2010. Identive Group, Inc. was founded in 1990 and is headquartered in Santa Ana, California.

Wave Systems Corp. develops, produces, and markets products for hardware-based digital security. Its products are based on the Trusted Platform Module (TPM), a hardware security chip that enables secure protection of files and other digital secrets, and performs critical security functions. The company offers EMBedded Application Security SYstem (EMBASSY) Trust Suite, a set of applications and services that are designed to bring functionality and user value to TPM enabled products. The EMBASSY Trust Suite includes the EMBASSY Security Center, Trusted Drive Manager, Document Manager, Private Information Manager, and Key Transfer Manager. It also offers middleware and tools, which include Trusted Computing Group (TCG) enabled toolkit that assists application developers in writing new applications or modifying existing ones to function on TCG-compliant platforms; and Wave TCG-Enabled Cryptographic Service Provider, which allows software developers to utilize the security of a TCG standards-based platform. In addition, the company offers EMBASSY Trust Server Applications comprising EMBASSY Key Management Server, a server application designed to provide corporate-level backup and transition of the TPM keys; EMBASSY Authentication Server that offers centralized management, provisioning, and enforcement of multifactor domain access policies; and EMBASSY Remote Administration Server, which provides centralized management and auditing of TPMs and self-encrypting drives. Further, it offers eSign Transaction Management Suite and broadband media distribution services. Wave Systems Corp. sells its products to chip original equipment manufacturers (OEMs), PC OEMs, enterprise customers, and systems integrators. The company was formerly known as Cryptologics International, Inc. and changed its name to Wave Systems Corp. in January 1993. Wave Systems Corp. was founded in 1988 and is based in Lee, Massachusetts.

Aware, Inc. supplies various products for the biometrics and imaging, and digital subscriber line (DSL) service assurance industries primarily in the United States and Germany. It provides biometrics software products, including software development kits (SDKs); software components; biometrics services platform to build and deploy server-based biometric data processing and workflow solutions; universal registration client (URC) that performs various biometric data capture, analysis, matching, formatting, and hardware abstraction functions; URC Mobile for performing biometric enrollment, identification, and screening on mobile biometric devices; FormScannerSE, FormScannerMB, and FormScannerSWFT for scanning and processing of inked fingerprint cards; Forensic Workbench for the categorization, processing, and standards-compliant formatting of biometric images and demographic data; and WebEnroll for browser-based enrollment of biographic data, fingerprints, and facial images. The company also offers medical imaging products comprising AccuRad ImageShare server, a software application for viewing medical images; AccuRad REM server to collect, store, and analyze radiation exposure estimation data; and AccuRad SDKs that implement image compression standards. In addition, it provides advanced imaging products, such as ArchivePack to store and distribute digital imagery; JPEG 2000 image compression software; and SeisPact for the storage and satellite transmission of seismic data from ships. Further, the company offers DSL service assurance products, including line diagnostics platform, a solution that enables broadband service providers to manage their DSL networks. Additionally, it provides engineering and software maintenance services, as well as licenses DSL chipset product line. The company sells its products through systems integrators and OEMs, as well as directly to end-users. Aware, Inc. was founded in 1986 and is headquartered in Bedford, Massachusetts.

IDEX ASA, a technology company, develops and supplies fingerprint imaging and recognition technology. It offers SmartFinger Film fingerprint sensor technology and sensor optimization algorithms that enable on device enrollment, template storage, and verification in the module. The company's SmartFinger Film sensor combined with footprint authentication software is suitable for various embedded applications, such as biometric tokens, biometric cards, remote controls, USB sticks, PC peripherals, locks, and handheld devices. It also offers a software development kit that enables customers to implement embedded fingerprint authentication solutions or add fingerprint authentication to existing products. The company provides SmartFinger technology to original equipment manufacturers and integrators as components for integration into products, or licenses the technology for imaging, hardware design, sensor chip solution, and software algorithms. Idex ASA was founded in 1996 and is headquartered in Fornebu, Norway.

Precise Biometrics AB provides biometric solutions to corporations and public organizations worldwide. The company operates in two segments, Mobile, and Identity and Authentication Management (IAM). The Mobile segment offers hardware, software, and services focusing on the mobile sector for smartphones and tablet PCs. This segment's solutions include Tactivo, a smart casing with a built-in fingerprint sensor and smart card reader to protect the information in smart phones and tablet PCs. The IAM segment offers a range of solutions, including embedded solutions for national ID cards, government agencies, banks, and companies. It offers fingerprint readers; Match-on-Card technology that enables the matching and storage of fingerprints on smart cards; and Precise BioMatch Embedded, a solution for integration in various hardware devices, including point-of-sales terminals, computers, and handheld units. This segment also provides physical access solutions for use in various premises, such as gyms with biometrics. In addition, the company offers consulting and integration services for its fingerprint recognition technology. It markets its solutions and products directly and via a network of partners, including smart card manufacturers, systems integrators, resellers, and hardware and chip manufacturers to countries, government agencies, corporations, and organizations. Precise Biometrics AB was founded in 1997 and is headquartered in Lund, Sweden.

Symantec Corporation provides security, storage, and systems management solutions to various organization and consumers worldwide. It operates in four segments: Consumer, Security and Compliance, Storage and Server Management, and Services. The Consumer segment provides Internet security for PC's, tablets, and mobile devices; services, such as online backup, online family protection, and remote help to individual users and home offices; and various free tools and services to consumers. The Security and Compliance segment offers solutions for endpoint security and management, compliance, messaging management, data loss prevention, encryption, managed security services, and authentication services; and solutions through its software-as-a-service (SaaS) and appliance security offerings. Its products enable customers to secure, provision, and remotely manage their laptops, PC's, mobile devices, and servers. The Storage and Server Management segment provides storage and server management, backup, archiving, eDiscovery, and data protection solutions in heterogeneous storage and server platforms; and solutions through its SaaS and appliance offerings. The Services segment offers consulting, business critical services, and education services to help customers address information security, availability, storage, and compliance needs. The company markets and sells its products through its direct sales force and eCommerce platform, as well as through distributors, direct marketers, Internet-based resellers, system builders, Internet service providers, wireless carriers, original equipment manufacturers, specialized partners, value-added resellers, large account resellers, managed service providers, system integrators, and in retail locations Symantec Corporation was founded in 1982 and is headquartered in Mountain View, California.

Palo Alto Networks, Inc. offers a network security platform in the Americas, Europe, the Middle East, Africa, the Asia Pacific, and Japan. The company's platform comprises Next-Generation Firewall that delivers application, user, and content visibility and control. It delivers its platform in the form of a hardware or virtual appliance, and includes a suite of subscription services, as well as support and maintenance services. The company's products include firewall appliances; Panorama, a centralized security management solution for the global control of appliances deployed on an end-customer's network as a virtual appliance or a physical appliance; and Virtual System Upgrades, which are available as extensions to the virtual system capacity that ships with the appliance. Its subscription services include threat detection and prevention, URL filtering, laptop and mobile devices protection, and malware and threats protection. The company also offers professional services, which include on-location planning, designing, and deployment of security solutions; application traffic management, solution design and planning, configuration, and firewall migration; and education services. Its platform enables enterprises, service providers, and government entities to identify, control, and safely enable applications running on their networks, as well as protect against cyber threats in real time. The company serves the enterprise network security market, which consists of firewall, unified threat management, Web gateway, intrusion detection and prevention, and virtual private network technologies. The company primarily sells its products and services through its channel partners, as well as directly to end-customers operating in various industries, including education, energy, financial services, healthcare, Internet and media, manufacturing, public sector, and telecommunications. Palo Alto Networks, Inc. was founded in 2005 and is headquartered in Santa Clara, California.

Verint Systems Inc. provides Actionable Intelligence solutions and value-added services worldwide. Its solutions are used to capture, distill, and analyze underused information sources, such as voice, video, and unstructured text. The company's Enterprise Intelligence Solutions segment offers a suite of enterprise workforce optimization and voice of the customer solutions and services, including Internet protocol (IP) and time division multiplexing voice recording, quality monitoring, voice of the customer analytics, workforce management, eLearning and coaching, performance management, and desktop and process analytics. Its Video and Situation Intelligence Solutions segment provides networked IP video and situation intelligence solutions, such as IP video management software and services; edge devices for capturing, digitizing, and transmitting video over various types of wired and wireless networks; video analytics; network video recorders; and physical security information management. The company's Communications and Cyber Intelligence Solutions segment offers solutions for communications interception, service provider compliance, mobile location tracking, open source Web and cyber intelligence, and tactical communications intelligence. This segment offers its products to law enforcement, national security, intelligence, and civilian government agencies to detect, investigate, and neutralize criminal and terrorist threats; and detect and thwart cyber-attacks. The company also offers implementation, consulting, and maintenance and support services. Verint Systems Inc. sells its products through its direct sales team; and through distributors, systems integrators, value-added resellers, and OEM partners under the Impact 360, Nextiva, RELIANT, VANTAGE, STAR-GATE, ENGAGE, FOCALINFO, and CYBERVISION brand names. The company was founded in 1994 and is headquartered in Melville, New York. Verint Systems Inc. is a subsidiary of Comverse Technology, Inc.

Sky-mobi Limited operates a mobile application store in China. The company works with handset companies to pre-install its Maopao mobile application store on handsets and with content developers to provide users with applications and content titles. The company's Maopao application store users can browse, download, and purchase various applications and content, such as games, music, and books. Sky-mobi Limited also offers mobile social games and social network functions, including instant messaging, blogging, personal profiling, content sharing, and virtual gifting on its Maopao Community. The company owns proprietary mobile application technology in the cloud computing, the MRP format, and SDK development environment. It has collaborative relationships with handset companies to embed its mobile application store for various types of mobile baseband, chipsets, and reference designs. As of March 31, 2012, it had approximately 977 million cumulative Maopao users; and cooperation agreements with approximately 860 handset companies. Sky-mobi Limited has a strategic alliance with SINA Corporation. The company was formerly known as Profit Star Limited and changed its name to Sky-mobi Limited in October 2010. Sky-mobi Limited was incorporated in 2007 and is based in Hangzhou, China.

Qihoo 360 Technology Co. Ltd. provides Internet and mobile security products in the People's Republic of China. Its principal products include 360 Safe Guard, an Internet security product for Internet security and system optimization; 360 Anti-Virus, an anti-virus application to protect users' computers against trojan horses, viruses, worms, adware, and other forms of malware; and 360 Mobile Safe, a security program for the Google Android, Apple iOS, and Nokia Symbian smartphone operating systems. The company's platform products comprise 360 Safe Browser, a Web browser; 360 Personal Start-up Page, a default homepage of 360 Safe Browser and a key access point to popular and preferred information and applications; 360 Application Store, a key access point to securely obtain and manage software and applications; and 360 Safebox, a solution that protects users against thefts of personal account information. It also provides online advertising services, including online marketing services and search referral services; and Internet value-added services comprising the operation of Web games developed by third-parties, remote technical support, and cloud-based services. Qihoo 360 Technology Co. Ltd. has strategic partnership with China Network Television. The company was formerly known as Qihoo Technology Company Limited and changed its name to Qihoo 360 Technology Co. Ltd. in December 2010. Qihoo 360 Technology Co. was founded in 2005 and is based in Beijing, the People's Republic of China.

NICE Systems Ltd., a software company, provides intent-based solutions that capture and analyze interactions and transactions, realize intent, and extract and leverage insights to deliver impact in real time. It offers a suite of enterprise customer interaction solutions comprising NICE SmartCenter to capture and analyze customer interactions across various communication channels, including phone, surveys, email, and Web; NICE Trading Suite that enables organizations to capture, monitor, and analyze interactions and transactions between traders, firms, and their counterparties; NICE Back Office Suite, which extends front office operational efficiency into back office processing environments; and NICE solutions for small and mid-sized contact centers and branch offices. The company also provides financial crime and compliance solutions through NICE Actimize, which offers real-time financial crime, fraud prevention, anti-money laundering, enterprise investigations, risk management, compliance, and trading surveillance capabilities to financial institutions, government agencies, and related organizations. In addition, it offers a range of security solutions for situation management, video surveillance and analytics solutions, public safety, and intelligence and law enforcement, which enable capture, analysis, and correlation of data from multiple sensors and systems, including audio, video, radio, geo-location, and Web. Further, the company provides business consulting, customization solutions, solution delivery, customer education services, and support and maintenance services. It sells its solutions and products directly, as well as through service providers, system integrators, distributors, value added resellers, and complimentary technology vendors to approximately 25,000 organizations in approximately 150 countries. NICE Systems Ltd. was founded in 1986 and is based in Ra'anana, Israel.

Nuance Communications, Inc. provides voice and language solutions for businesses and consumers worldwide. It provides dictation and transcription solutions and services that provide platforms to generate and distribute clinical documentation; clinical documentation improvement programs; and speech recognition solutions for radiology, cardiology, pathology, and related specialties enabling healthcare providers to dictate, edit, and sign reports without manual transcription. The company also offers mobile and consumer solutions and services comprising an integrated suite of voice control and text-to-speech solutions; dictation applications; predictive text technologies; mobile messaging services; and dictation, Web search, and voicemail-to-text services for use in phones, cars, tablets, desktop and portable computers, personal navigation devices, and other consumer electronics. In addition, it provides customer service business intelligence and authentication solutions, such as speech recognition, natural language understanding, text-to-speech, biometric voice recognition, and analytics for enterprises in the telecommunications, financial services, travel, entertainment, and government sectors to support, understand, and communicate with their customers. Further, the company offers document imaging, print management, and PDF solutions to multifunction printer manufacturers, home offices, small businesses, and enterprise customers; and software development toolkits to independent software vendors, as well as licenses its software to multifunction printer manufacturers. Nuance Communications, Inc. markets and sells its products through direct sales force and a network of resellers, as well as through its e-commerce Website. The company was formerly known as ScanSoft, Inc. and changed its name to Nuance Communications, Inc. in October 2005. Nuance Communications, Inc. was founded in 1992 and is headquartered in Burlington, Massachusetts.

About Us

Disclaimers