

RESEARCH NOTE: STRIKEFORCE TECHNOLOGIES, INC.

IMPROVED CONSUMER SECURITY AND NEW TECHNOLOGIES ARE GROWING THROUGH CRISIS & MANDATE

[OTCBB: SFOR \$0.015]

Research^{2.0}

Boston | New York | Paris

Kris Tuttle & Stephen Waite
February 22, 2012

SUMMARY

Most enterprises were forced to reevaluate their security in 2011 after a tidal wave of major security breaches and new mandates for firms in financial services. Most are now in the implementation stages, which is allowing some smaller companies to take share from the large established players. In particular, anything that doesn't use multiple factors and so-called "Out-of-Band (OOB)" techniques is suspect. It's now clear that keystrokes need to be encrypted to avoid hijacking of user data streams and online sessions.

We are shifting away from logins, RSA tokens, anti-virus scanning and challenge questions to multi-factor security and the use of Out-of-Band (OOB) methods. At the same time, mobile devices are quickly becoming the primary end-user access point. Mobile device management with improved security is one of the hottest categories in 2012 enterprise IT spending. User protection and data loss prevention are a top priority.

StrikeForce Technologies, Inc. (StrikeForce) is one of a handful of small innovative companies delivering the leading solutions for multi-factor and out-of-band authentication. Although other companies are spending more on marketing, StrikeForce developed some of these key technologies long before others and have secured a key patent on OOB authentication with other patents pending.

The most surprising thing about StrikeForce is that for a tiny company they have the best enterprise scale solution for user authentication and data loss prevention. This is partially explained by their management team which includes the CTO steeped in information security and a former staff member at Bell Labs and the CEO who was a CIO of JPMorganChase. Our discussions with customers repeatedly back up their enterprise advantage.

One emergent theme from our work in this space is that the combination of both strong encryption and OOB methods is what is really needed to secure user access and prevent data loss. StrikeForce is the only company currently delivery this combination of technologies into the enterprise environment.

Included in our report are some survey results from a recent Aberdeen report¹ highlighting this area as something they are seeing increasingly in their day-to-day research inquiries and surveys. Not only is OOB at the top of their "interest index" but they also note the importance of the StrikeForce patent. Another recent study by TheInfoPro concluded that spending on Mobile Device Management (MDM) is the strongest segment of network security and services.²

StrikeForce is poised for a strong 2012 on the back of a number of major customer wins in financial services, expanded distribution agreements and new products that will be previewed at the upcoming RSA conference in late February. We believe StrikeForce is an important technology asset that is growing in value in an undeniably expanding area. The current public market value of the company is only a fraction of our estimate of intrinsic value.

Next week StrikeForce will be presenting at the American Growth Capital and then showing off some new technology offerings for the Apple OS and mobile devices like the iPad at the big RSA security conference.

¹ Analyst Insight: **The Case for Phone-based Authentication: Jumping on the Out-of-Band Wagon**, Aberdeen Group, December 2011.

² Networking Real-Time Update, November 2011, TheInfoPro (now part of 451 Research).

The rest of this report provides a more detailed overview of the market background, StrikeForce products and company positioning, market opportunity, and a closer look at valuation and the ecosystem.

BACKGROUND

Data security has become a very hot issue thanks to a series of large-scale data breaches, including breaches at Sony, Epsilon, Citibank, and RSA. The problem is pervasive and there are meaningful (but not headline-grabbing) data breaches on a daily basis.³ Intel CEO Paul Otellini summed things up succinctly when he stated, *“The importance of security has never been greater.”* We suspect that many of those who are responsible for information security at Fortune 1000 companies and large government agencies are telling their bosses the same thing. Things have evolved to the point today where the hackers have begun hacking the hackers, and they are even advertising the fact! And while talk of “cyber wars” between nations was the stuff of science fiction novels in the 20th century, today it is a reality and, as the recent *Bloomberg Businessweek* cover story noted, there is an emerging cyber-weapons industry evolving to arm the combatants.⁴

The growing importance of information security, both in the U.S. and globally, is a reflection of the growth in the usage of the internet and e-

commerce. Internet usage has soared nearly 500% over the past decade. Today, over 2 billion people use the internet, or almost one-third of the total world population.⁵ With more and more people using the internet, online commerce has mushroomed. E-commerce sales in the U.S. rose to \$165 billion in 2010, up nearly 15% from \$144 billion in 2009. Sales online are growing at a faster pace than U.S. retail sales overall and are becoming a larger share of total retail sales. That said, online commerce in the U.S. is still less than 5% of total retail sales. There is considerable room for growth in the years ahead with the ongoing expansion of social networking and the proliferation of smart phones, iPads, tablets, and the like.

Authentication has always been important in information security, and is becoming even more critical today, especially with the latest regulations in the financial industry which now calls for Out-of-Band Authentication as a necessary additional level of security, and the need for

products that stop keylogging malware, the fastest growing means of identity theft and data breaches. Anti-virus and anti-spyware technologies have

Costly Security Threats on the Rise

RSA Hack Demonstrates Superiority of Cell Phone as 2nd Factor: In March, 2011 information security vendor RSA (part of EMC Corp.) disclosed that they had been the victim of an “APT” (Advanced Persistent Threat), a fancy term for “We were hacked.”

Emerging Social Networking Security Threats: Facebook, with over 700 million accounts, is the new frontier for fraud. In the past year, social networks have soared to 4th from 17th as the most treacherous web terrain, behind porn and software sharing sites.

Cyberattacks against federal networks on the rise: The number of attacks against federal networks increased nearly 40% last year, according to a White House report to Congress on federal computer security.

Cost of Identity Theft-related Fraud: The average amount of loss (cash and goods) per fraud for identity theft is over \$10,000. The estimated total business loss associated with identify theft is over \$33 billion and counting.

³ For those who have an interest in following security breaches can spend some time at www.privacyrights.org to learn more.

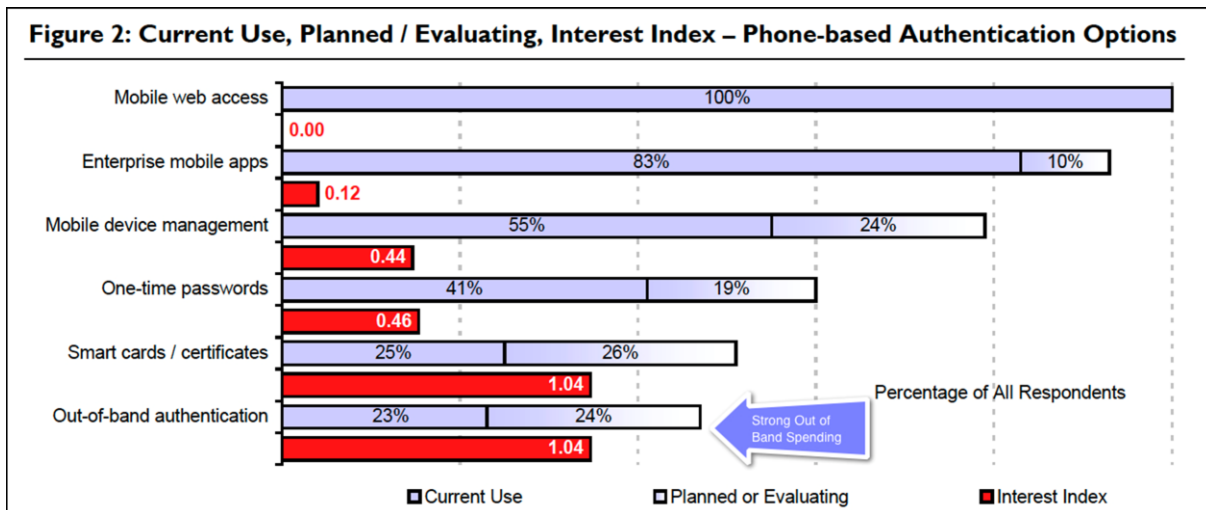
⁴ <http://www.businessweek.com/magazine/cyber-weapons-the-new-arms-race-07212011.html>.

⁵ Internet Usage Statistics, <http://www.internetworldstats.com/stats.htm>.

been key pieces of the information security equation for quite some time. Infections are rampant on the web. A new infected website is discovered every 3.5 seconds (almost 24,000 every day).

As internet usage continues to grow and become pervasive, there are emerging security issues that are presenting great challenges for consumers, enterprises and regulators. Over the past couple of years, we have seen malicious software designed to steal online usernames and passwords skyrocket – both in volume and level of sophistication. In

agencies' supervisory expectations regarding customer authentication, layered security (including Out-of-Band Authentication and solutions to stop keylogging malware), and other controls in the increasingly hostile online environment. The FFIEC notes that customers and financial institutions have experienced substantial losses from online account takeovers. Effective security is essential for financial institutions to safeguard customer information, reduce fraud stemming from its theft, and promote the legal enforceability of financial institutions' electronic agreements and transac-



Source: Aberdeen Research

addition, new so-called Trojan horses have been discovered (e.g. Zeus) which can steal money from bank accounts and post fake balances. If that weren't enough, we have seen the proliferation of keylogger malware programs can record everything a person types on their computer without their knowledge and transmit it all back to those trying to steal information.

Given that many online perpetrators are interested in obtaining login information that allows access to consumer and business banking data, we are seeing the emergence of new regulatory guidelines in the U.S. financial services and health care industries. The Federal Financial Institutions Examination Council, FFIEC, issued a supplement last year to the *Authentication in an Internet Banking Environment* guidance that was released in October 2005.

The purpose of the supplement is to reinforce the risk-management framework described in the original guidance and update the FFIEC member

tions.

Importantly, the FFIEC supplement stresses the need for performing risk assessments, implementing effective strategies for mitigating identified risks, and raising customer awareness of potential risks. It stops short of endorsing any specific technology for doing so. The FFIEC member agencies stated they will continue to work closely with financial institutions to promote security in electronic banking from now on, and have directed examiners to formally assess financial institutions under the enhanced expectations outlined in the supplement.

Similar security updates have been incorporated with the latest Health Insurance Portability and Accountability Act (HIPAA) regulation for the healthcare industry, requiring many of the same strong guidelines and stressing the need for performing risk assessments, implementing effective strategies for mitigating identity risks and suggest-

ing strong two-factor authentication and solutions to help protect against malicious malware.

The growing importance of information security for consumers, enterprise and governments represents an opportunity for companies providing innovative and trusted security software. Over the past several years, we've seen a great deal of consolidation in the information security sector. EMC's acquisition of RSA highlighted the growing importance of security in the enterprise. Intel's recent acquisition of McAfee took many analysts and observers by surprise. The message from Intel on its acquisition of McAfee was clear: the importance of security has never been greater. Recently, we have seen a growth spurt in venture-backed information security companies, with some companies raising private and public capital (e.g., Imperva, Tangoe, AVG, Trustwave, and Proofpoint).

STRIKEFORCE TECHNOLOGIES

One of the emerging information security vendors flying below the radar screen is StrikeForce. StrikeForce is a security software development and services company that offers a suite of integrated computer network security products. Founded a decade ago and headquartered in Edison, New Jersey, StrikeForce Technologies has developed proprietary security technology solutions for consumers, enterprise and government agencies. StrikeForce is led by three experienced executives: Mark L. Kay, Chairman & Chief Executive Officer; Ram Pemmaraju, Chief Technology Officer; and George Waller, Executive Vice President in charge of Sales and Marketing.

StrikeForce has been developing security technology for years but well ahead of the market demand curve. StrikeForce's two core products, ProtectID and GuardedID, have entered mainstream adoption in just the last 18 months.

There are many information security companies in the market today serving consumers, enterprises and governments. StrikeForce has the most fully featured solutions for both Out-of-Band authentication and real time anti-keylogging encryption technology. As mentioned above, the company has two core product offerings today: ProtectID and GuardedID. ProtectID is StrikeForce's Out-

of-Band authentication technology and GuardedID is the company's real time anti-keylogging encryption. Due to rising security threats online, both technologies are becoming necessities for internet users today. In the section that follows, we take a closer look at each technology.

PROTECTID: A SECURE AUTHENTICATION PLATFORM

StrikeForce's ProtectID product is a complete platform that provides customers "Out-of-Band," phone, soft and hard token options all at the same time, as well as biometric capabilities. ProtectID's Out-of-Band authentication platform provides state-of-the-art authentication flexibility. It is analogous to the long-established concept of out-of-channel signaling developed by telephone network providers that was used to stop the theft of service in the form of free telephone calls and network usage, and to improve operational efficiency. The out-of-channel signaling developed by telephone network providers, such as AT&T, has proven extremely effective and is widely used today by every major provider of voice services on the Public Telephone Switched Network. StrikeForce uses the same principle as the basis for its proprietary patented ProtectID Out-of-Band authentication platform.

The Out-of-Band process used makes it far more difficult to steal vital and important information (e.g. password to a bank account). Rather than logging in key information "In-Band" through a computer, users go offline or Out-of-Band through a separate, more secure channel (typically a landline telephone or mobile phone).

A major security flaw exists in the current use of the same (physical and logical network) channel for the processing of a user's identifier (the User ID or username) and what they know (their Password). When a user accesses a computer, he/she is asked to authenticate or prove their identity via a simple login process (username and password, token or certificate), or alternatively through the use of a complex technology process such as a biometric verification (voice, fingerprint, iris, etc.). The authentication information is sent via the same network used to access the computer. Because the information is sent over the same net-

work, it is “in-band.” Since most computers in the world are connected to the internet, either directly or indirectly, a hacker who has access to the internet (from anywhere in the world) can potentially access any other computers linked through the internet. Furthermore, since all authentications are “In-Band,” a potential hacker is given the accessibility to break in to an account and steal.

login screens or wherever an authentication is required prohibits hackers from running password “cracking” programs that can discover an individual’s identity. By addressing these two key network authentication security issues, StrikeForce’s proprietary authentication technology and process significantly inhibits the ability of internet hackers to gain access to the business or personal compu-

StrikeForce’s ProtectID Platform versus the Competition

	StrikeForce	Authenticate	PhoneFactor	Validsoft	Swivel
Hard Token	X				
Soft Token	X		X		
OOB Authentication	8 methods	few methods	few methods	few methods	few methods
Transaction Verification	X	X		X	
Cloud Service	X	X	X	X	
On-Premises	X				X
Redundant Authentication	X				

Serious security-related problems can arise with In-Band authentication security technology as everything functions within the same linear band (i.e., the internet).

ProtectID solves two network authentication security flaws. The first is that security related information can be stolen from the IP Network. The ProtectID platform resolves this “sniffing” flaw by using the platform’s Out-of-Band capability and providing a separate pathway outside of the computer for sending the password, thereby removing the password from the internet or computer being monitored or stolen. The second flaw in network authentication is the availability of the “password” input field to the hacker. If the hacker can access the input box, a “password cracking” program can be initiated.

The ProtectID platform resolves this flaw by removing the input field completely from the login screen. The removal of a password input field on

login screens or wherever an authentication is required prohibits hackers from running password “cracking” programs that can discover an individual’s identity. By addressing these two key network authentication security issues, StrikeForce’s proprietary authentication technology and process significantly inhibits the ability of internet hackers to gain access to the business or personal compu-

ting accounts of an individual through attacks on a user’s login or any transaction password.

ProtectID is built to use a variety of Out-of-Band communication methods, including cellular/wireless and landline phones using PIN or OTP, One Time Password (OTP) physical Token, OTP soft Tokens on Blackberry, iPhone, iPad, Droid, other PDAs or Phones with application capability, OTP on a computer through a desktop client or email, smart cards, web authentication, domain authentication through a ProtectID Microsoft modified logon (Gina), as well as other methods. The ProtectID platform is flexible and can be used for many applications, including secure website logon, single sign-on products, corporate VPNs, LAN Domain authentication, Citrix application authentication, secure application authentication, Oracle’s OAAM, CA’s Siteminder Single Sign On and others, transaction verification, password reset, and full redundancy.

StrikeForce offers customers the flexibility to have ProtectID installed in-house or be processed through their Cloud Authentication Service (CAS). StrikeForce completed the development of its ProtectID platform at the end of June 2004. Early in 2011, the company was awarded a broad patent from the U.S. Patent and Trademark Office on its Out-of-Band authentication process, thereby strengthening the company's competitive position in the information security market. The patent comes at an important time when large, established corporations are dealing with costly data breaches and stronger regulations, and who are looking for more secure alternatives. The patent went through reexamination and came out in December of 2011 without losing any claims and even adding 7 more.

In speaking with several of StrikeForce's authentication customers, there was a high level of overall satisfaction with ProtectID. Customers – some of whom have been using the product for years – noted that the product is effective at providing high-level authentication security and is at a price point that is attractive relative to the competition. There are several companies in the market offering competing authentication products, including Authentify, Phone Factor, Swivel, ValidSoft, Verisign, and RSA.

The exhibit previous shows how ProtectID stacks up against the competition in terms of features and flexibility. One can see that StrikeForce's offering is broader and deeper with greater flexibility and choice relative to the competition. The fallout from RSA's woes following the hacking of their proprietary security encryption code has been sig-

nificant and StrikeForce is in a position to gain from companies that are searching for alternative secure authentication solutions.

GUARDEDID: ANTI-KEYLOGGING

The Problem with Conventional Security Software

All anti-spam and anti-virus tools are based on scanning a computer for files with a particular signature. The databases containing signatures of known bad files have to be continuously updated. The major caveat in this approach is the existence of the signature of a known problematic file. Spammers and criminals are currently deploying sophisticated software which dynamically changes the file signature. Therefore, anti-spam tools are no longer effective against keyloggers. Also, there is significant time between detecting a new keylogger on the internet and the anti-keylogging signature being updated on anti-virus/spyware software. This time gap can be a month or more.

Some of the anti-keylogging software prevents Windows hooks from being used by keyloggers (Windows hooks are used by keyloggers to spy on keystrokes sent from the keyboard to the application). However, they are not always effective and can be circumvented in most cases by keyloggers.

Another key piece is security technology that encrypts your keystrokes and prevents keylogging malware in real-time. StrikeForce has developed a technology called GuardedID that provides protection to consumers, enterprises and governments against keylogging malware. Malware (short for malicious software) has become a serious problem throughout the world.⁶ Earlier this year, Microsoft stated that 1 out of every 14 downloads (7%) leaves malware on the client computer. Malware is a global problem, and it appears that the source of much malware is overseas. Last year, information security company Symantec cited Shaoxing, China as the world's malware capital.

Conventional anti-virus software solutions on the market today claim protection against malware, but these claims are misleading given the virulent and diverse nature of malware. The fact is many, if not all, of the popular anti-virus software products on the market are inefficient in protecting users against serious and costly forms of malware, such as keylogging malware, especially "zero day" at-

tacks. These are attacks that occur in real time.

⁶ Software is considered to be malware based on the perceived intent of the creator rather than any particular features. Malware includes computer viruses, worms, Trojan horses, spyware, dishonest adware, scareware, crimeware, most rootkits, and other malicious and unwanted software or programs.

Keylogging is a malicious breed of malware. Often invisible to users, keylogging malware sends vital information such as passwords and credit card numbers from a computer to perpetrators whose main intent is to plunder. A keylogger can also record instant messages, e-mail, and any information a user types into a computer at any time. Given that keyloggers are viewed as the top security threat today, there is a growing need for anti-keylogging software such as StrikeForce's GuardedID product.

GuardedID fills an important gap in the information security market today. Unlike anti-virus software used today, GuardedID is the only product that provides three critical security functions that are necessary for a secure computing environment. GuardedID provides users with:

- Secure keystroke encryption
- Out-of-Band, in-client computer processing for identity protection
- Real-time keylogging malware prevention

StrikeForce initiated the core development of GuardedID back in late 2006 and has a patent pending on the software with the U.S. Patent Office. StrikeForce has a unique approach to provide security against malicious keyloggers. GuardedID takes a preventative approach rather than trying to detect keyloggers. It takes control of the keyboard at the lowest possible layer in the kernel. The keystrokes are subsequently encrypted and sent to the browser or the application via an Out-of-Band channel in the client computer, thereby bypassing the Windows messaging queue (it should be noted that GuardedID is available today only for computers running Windows; a version of GuardedID for Apple computers is currently in development and expected to be on the market in the near future).

A key feature of GuardedID is a built-in self-monitoring capability. It encrypts all entered key data in real time and prevents hackers from stealing important user information. GuardedID creates a separate channel for delivering keystroke data to the application message queue. By doing so, it prevents the keystroke data from being bypassed by other software. Importantly, if GuardedID is tampered with in any way by a would-be hacker, it

will alert and warn the user of a potential breach. Another feature of GuardedID is a unique method StrikeForce calls "CryptoColor®" to indicate to the user that the software is working and the user input is secured. The colored text box into which users enter data provides strong visual feedback that they are operating in a secure environment. In those cases in which GuardedID is not able to secure user input, GuardedID warns users that encryption is off by changing the color of a status button on the GuardedID toolbar.

GuardedID is also effective against a new security vulnerability known as clickjacking. Web coding allows a single web page to be constructed from different items (ads, images, links, etc.) in "frames." Typically, the frames all come from a single domain (e.g., guardedid.com), but they may come from other domains (ad servers, media servers, etc.). Clickjacking uses this normally helpful feature to trick users by showing the expected web page but overlaying or underlaying some other unexpected page from a different domain, usually attempting to steal money or credentials. As a result, a web page can have a hidden frame that contains a clickable button that can invisibly hover below the user's mouse. Thus, when the user clicks the mouse, they unintentionally click the invisible button. This results in an undesirable action, such as downloading malware, transferring money or purchasing something inadvertently.

One solution used to deal with clickjacking is disabling JavaScript. However, this act drastically reduces the usability of the computer and disrupts the internet experience. GuardedID incorporates a different approach to protecting users from clickjacking, warning the user when content is not from the same domain. If false content is hidden in an invisible overlay, GuardedID makes it visible. If the content is hidden underneath, GuardedID highlights it by drawing red borders around it. With GuardedID, users are fully aware of all content on the webpage, and thus alerted to any potential clickjacking activity.

StrikeForce offers GuardedID in three different versions: Standard, Premium and Enterprise. The Standard version is targeted at consumers. It secures a user's entire internet experience. This version requires the user to download and install the GuardedID toolbar into their internet browser.

GuardedID is automatically launched every time Internet Explorer and Firefox browsers are opened for any type of online activity. The Premium version secures a user’s entire internet experience as well as almost all Windows applications (e.g., MS Office, Google Chrome, IM/chat, financial/accounting applications and many other applications). The Enterprise version offers protection to all employees and covers all activities, whether on a corporate network or working remotely with Enterprise administration rights.

There are several companies offering products that compete with StrikeForce’s GuardedID, including Trusteer, Sentry Bay, Key Scrambler, and SafeCentral. As the exhibit below shows, GuardedID offers consumers, enterprises and governments complete security against malware relative to its competitors in the market today. GuardedID is the only product that can protect all applications on your client computer with continuous visual reinforcement, a feature clients provide positive comments about.

StrikeForce’s other partner, Intersections, is a public company (NASDAQ: INTX) that provides a set of comprehensive tools to consumers directly and via partnerships with financial institutions. Intersections views GuardedID as the best anti-keylogging product on the market today. Intersections uses the additional security of GuardedID to differentiate their security and identity management solution from other companies like LifeLock.

We expect Intersections to continue to be aggressive with marketing since they enjoy much greater profitability when they go direct to consumers. With trailing revenues of \$370M, the company has substantial resources to continue to expand their reach and spread StrikeForce’s GuardedID at the same time.

MARKET OPPORTUNITY AND STRATEGY

There is little question that the importance of information security has never been as great as it is

	StrikeForce	Trusteer	Sentry Bay	Key Scram	SafeCentral
Anti-Keylogging	X	X (limited)	X	X	X
Anti-Clickjacking	X				
Anti-Screen Capture	X	X	X		X
Prevent MITM Attack	X	X			
Online Security	X	X(limited)	X	X	X
Desktop Security	X			Partial	
Deployment Mgmt	X				

Discussions we had with several of StrikeForce’s customers and partners revealed an extremely high level of satisfaction with GuardedID. StrikeForce has partnered with WhiteSky (IDVault) and Intersections (Identity Guard, Total Protection and Privacy Protect) to make GuardedID widely available to major corporations and consumers. WhiteSky has embedded GuardedID into a consumer offering that is provided as part of the Comcast consumer offering. As the number of users expands it brings incremental revenue to StrikeForce.

today. With the number of internet users expected to continue growing beyond 2 billion, and ample room for an expansion of e-commerce in the global economy, one can easily argue that information security will only gain in importance in the future. There may be only two certainties in this world – death and taxes – but if there is a third, it is that computers will be hacked.

Hacking in all of its forms has become a vast illegal enterprise today. According to the U.S. Federal Bureau of Investigation, revenues from cyber-related crimes rival the illegal drug trafficking

business, with profits exceeding \$1 trillion. Meanwhile, the cost of identity theft in the U.S. has been estimated to exceed \$50 billion. The experi-

StrikeForce has a current addressable market opportunity of \$150-200 million per year that is growing at 15%.

ence of the past year with a growing number of high-profile hacking incidents suggests to us that there will be an even greater focus on information security by consumers, businesses and governments than anything we have seen in the past.

Authentication/identity management has historically been something of an orphaned stepchild in the world of enterprise information security. That relationship appears to be now changing, and there are signs that the relationship between information security concerns and authentication/identity is becoming more intimate today, creating new market opportunities. The tighter relationship between identity management and information security in the enterprise is related directly to the challenges presented by the transformation of the threat environment – which, as noted above, has become ever more treacherous and costly. The high profile security attack associated with RSA’s authentication technology earlier this year has created a favorable dynamic in the market for companies like StrikeForce with its more secure Out-of-Band technology. Those companies that can demonstrate a more secure authentication technology in the wake of the RSA hacking incident are likely to have a much larger audience today than otherwise, especially when they are also selling at a lower price point.

Regulation and compliance is also becoming an important driving force in the market for information security technology. Multiple U.S. government regulations (e.g., FFIEC, HIPPA) and mandates now require “two” factor authentication – that is, something stronger than just password authentication. Needless to say, the costs of insecure authentication technology are potentially astronomical for enterprises and organizations operating in the financial services and health care sectors. The market for information security technology is also being buffeted by the growing popularity of social networking sites and the cloud. Social

networking and cloud computing are exposing internet users to new forms of malicious security attacks. The security threats from the expansion of social networks and the cloud are bringing keylogging into greater focus today as a major potential security threat. A recent report by Verizon cited keylogging as one of the top five causes of data breaches and identity theft.

The worldwide market for security software totaled \$16.5 billion in 2010, which was up 12% from 2009⁷. Based on the preliminary data we have seen, this growth has accelerated in 2011.⁸ StrikeForce has some best-of-breed technology and significant relationships to build their position in this growing segment of authentication, identity management, and keylogger prevention software. The company’s target markets include:

- e-Commerce companies (payment processors, ISP’s, retail companies)
- Cellular carriers (VPN Managed Services, internal utilization)
- Financial firms (banks, brokerages, insurance companies)
- Technology Software companies
- Government (School/College systems, Local/State/Federal agencies) & Military
- Healthcare industry (HIPPA compliance critical)
- Bundled security packages

StrikeForce products participate in almost all segments of the security market. Performance, price, ease of use, security effectiveness, technical features, manageability, scope of product offerings, brand name, distribution channels, and customer support and service are the key competitive factors. In our discussions with partners and customers, StrikeForce’s products rate highly on many of these important elements.

So what is the real market opportunity for StrikeForce? We’d break it into two categories, one for authentication and one for anti-keylogging. Authentication is an established mar-

⁷ Gartner Group, June 7, 2011.

⁸ The InfoPro Quarterly Update, July 8, 2011.

ket. Market leader RSA (a division of EMC) has revenues of over \$500m. We put the annual recurring revenue opportunity for StrikeForce authentication products in the \$50m to \$100m range.

Anti-keylogging is a much newer segment of the security software market and it's not yet well recognized or understood by average consumers. We believe this is going to change and shift attention from anti-virus techniques to more proactive methods like anti-keylogging. According to IDC, 425m desktop/laptop computers and 500m smartphones and tablets will be shipped in 2011. Even using relatively low pricing of \$10/year for computers and \$5/year for devices, the gross market opportunity for anti-keylogging software is massive. However, we all know that only a portion of those devices will adopt the technology. There is a price elasticity issue as well, particularly on the OEM side. Dell probably wouldn't bundle a solution for \$10/computer but they probably would for \$1/computer.

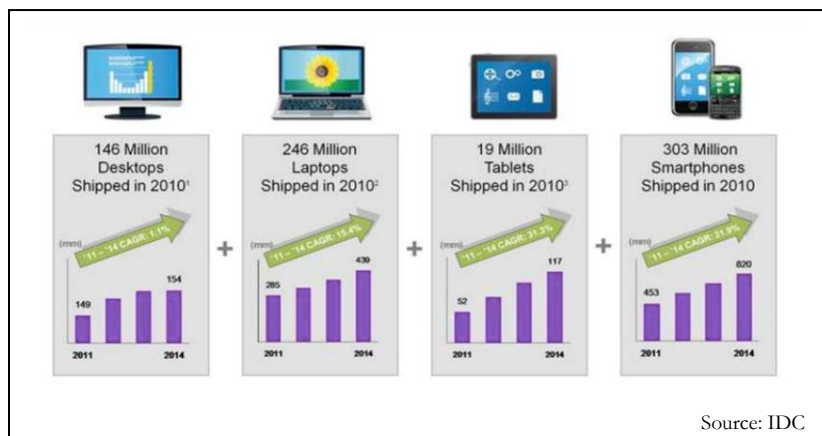
For our estimate we are going to use some industry standard metrics: 30% of the user population will be interested enough to download or try this feature, and 10% of those will be willing to pay for it. These are figures we see new services gravitate to over time. The math works out simply to 3% of 925m units covered, or 28m computers and devices. Based on what we have seen, we think StrikeForce can capture half of that market at a blended ASP of \$7/unit/year or \$100m/year in recurring revenue that will continue to grow each year.

Combined, this provides StrikeForce with a current addressable market opportunity of \$150-200 million per year, and growing at 15%.

StrikeForce has a multi-channel sales strategy that gives it global reach. StrikeForce sells its proprietary security software globally to consumers, enterprises and governments through OEM partnerships with other security technology vendors such as WhiteSky/ID Vault and Intersections/Privacy Protect, as well as other distribution channels that include resellers, distributors, and direct. Additionally, StrikeForce works with Vasco (VDSI),

who manufactures the One Time Password (OTP) hard token for ProtectID customers that prefer a physical token.

The typical sales cycle for StrikeForce is 3 to 6 months, although direct sales can be accomplished in a shorter time frame, typically 1 to 3 months. Pricing varies by target customer, product and usage. The company's business model is a standard software model based on subscriptions and maintenance fees. StrikeForce's pricing strategies provide appreciable discounts to consumers, corporate users and partners with access to the strong authentication protections offered by the ProtectID platform as compared to the pricing schedules of RSA's SecureID (main authentication competitor). There are also appreciable discounts



available for first-time users of GuardedID keyboard encryption technology.

Users who access ProtectID through the cloud pay monthly recurring fees based upon monthly transaction volumes. The transaction fee structure is also used with OEM contract arrangements for large one-time fees associated with licensed assignment of rights to the technology. The cost per transaction can start as low as \$0.02 and go as high as \$0.29 depending on the method of authentication and volume. For small and medium sized enterprise customers, there are one-time license fees for a set number of years, typically three or more, with an ongoing maintenance fee of 18% due up front each year. The fees for ProtectID start at around \$25 for ProtectID Phone including OTP and approximately \$60 with Physical Token, with volume discounts available. Maintenance for the ProtectID software is set at 18% of the contracted pricing.

Pricing strategies for GuardedID vary by customer and setting. GuardedID is typically purchased as a one-, two- or three-year subscription with discounts if multi-year licenses are purchased in advance for the enterprise. Renewals are based upon expiration date and are discounted accordingly. The Retail Manufacturers' Suggested Retail Price for GuardedID is \$39.99 with a \$10.00 immediate discount. StrikeForce grants price and quantity discounts in order to remain very competitive in the market. The company maintains a shopping cart hosted through Element 5 (Digital River) for the purchase of the GuardedID product by consumers and small to medium sized businesses. This shopping cart is also used by StrikeForce's global and domestic affiliates who maintain links on their websites to resell its products.

As the heavy discounting associated with the pricing of ProtectID and GuardedID suggest, the market for information security software is highly competitive. We view StrikeForce's near term fortunes as being closely tied to their OEM partnerships and the future performance of those partnerships. In our discussions with WhiteSky and Intersections, both companies have embarked on strategies to drive greater visibility and sales of StrikeForce's products. As noted earlier, WhiteSky is packaging StrikeForce's GuardedID as a standalone product and is rebranding it in the market as "Keystroke Defender." Meanwhile, Intersections is becoming more aggressive in introducing its customers in the financial services industry and elsewhere to StrikeForce's products.

VALUATION AND SUMMARY

Due to their small size and undercapitalization, StrikeForce trades quietly over the counter. The timing for a recapitalization of StrikeForce is at hand given the current end market dynamics and the technology and customer assets the company is building in both Out-of-Band authentication and anti-keylogging software.

The company basically doubled revenue levels in 2011, will do so again in 2012 and can do so for the next few years given their small size. Our projected 2012 revenues are just over \$1M with ap-

proximately \$800K of that revenue estimate is visible in the form of recurring revenues.

Our IV model for StrikeForce assumes expanding gross and net margins to relatively high levels that are consistent from a subscription and maintenance fee-based business model that leverages global OEM partnerships to drive sales growth. The IV estimate of \$19M for the company equals \$0.08/share.

In summary, StrikeForce is at a critical juncture today. The outlook for the company's core products has brightened considerably over the past year amid high profile data breaches and costly hacking incidents that are causing consumers, enterprises and government to reassess their security technologies and needs. With market adoption in full swing – as evidenced by tightening compliance and regulatory guidelines mandating more secure information systems – it would appear that it is prime time for StrikeForce's Out-of-Band authentication and anti-keylogging technologies.

It is incumbent now upon management to execute on the emerging opportunities in the marketplace. The company's security technology is first-class and well respected by partners and current customers. Execution on the operating side of the business will be key for StrikeForce along with financial restructuring.

On a final note, followers of and investors in information security companies know very well there has been a great deal of consolidation during the past decade through M&A activity. Whether StrikeForce is a suitable acquisition candidate to a bigger, more established information security company remains to be seen. Whatever the case, there is little reason not to expect further consolidation of the information security sector in the months ahead as security vendors seek to diversify and broaden their product offerings to customers.

STRIKEFORCE IV MODEL

StrikeForce

SFOR

2/22/2012

Base Case

Dec YE	2009	2010	2011	2012	2013	2014	2015	2016	SFOR	Ticker
YoY Change \$		-\$0.1	\$0.2	\$0.6	\$0.9	\$1.0	\$1.5	\$1.5	OTCBB	SFOR
Total Revenue	\$0.4	\$0.3	\$0.5	\$1.1	\$2.0	\$3.0	\$4.5	\$6.0	56%	Rev Growth
YoY Growth		-35%	80%	129%	82%	50%	50%	33%	\$0.01	Current Price
COGS %	22%	15%	15%	12%	9%	8%	7%	6%	230	Shares Out
COGS \$	\$0.1	\$0.0	\$0.1	\$0.1	\$0.2	\$0.2	\$0.3	\$0.4	4%	Avg. Dilution
Gross Profit	\$0.3	\$0.2	\$0.4	\$1.0	\$1.8	\$2.8	\$4.2	\$5.6	\$3.2	Cap (M)
Gross Margin	78%	85%	85%	88%	91%	92%	93%	94%	\$0	Cash
SG&A %	nm	nm	50%	40%	35%	30%	25%	22%	\$4.0	LT Debt (M)
SG&A	\$1.8	\$1.1	\$1.1	\$1.1	\$1.2	\$1.3	\$1.4	\$1.5	35%	Tax Rate
R&D %	102%	151%	20%	25%	25%	25%	25%	25%	17.5	P/E Multiple
R&D \$	\$0.4	\$0.4	\$0.10	\$0.28	\$0.50	\$0.75	\$1.13	\$1.50	15%	Discount Rate
Operating Margin	nm	nm	-193%	-42%	7%	26%	40%	47%	\$0.08	Intrinsic Value
Operating Income	(\$1.89)	(\$1.24)	(1)	(0)	0	1	2	3	492%	Up/Downside
Other Income	-0.6	-1.6	-1.0	0	0	0	0	0		
Taxes	(0.25)	0.00	(0)	(0)	0	0	1	1		
Tax Rate	35%	35%	35%	35%	35%	35%	35%	35%		
Net Income	-\$2.24	-\$2.87	-\$2	\$0	\$0	\$0	\$1	\$2		
Net Margin	nm	nm	-315%	-24%	4%	15%	24%	29%		
Market Value Using P/E	-\$39	-\$50	-\$26	-\$5	\$1	\$8	\$19	\$30		
Cash Position	\$2	\$4	\$0	\$0	\$0	\$1	\$2	\$3		
Shares (M)	99	168	215	230	239	249	259	269		
Period Share Price	\$0.00	-\$0.30	-\$0.12	-\$0.02	\$0.01	\$0.03	\$0.07	\$0.11		
PV of MV 4 Years Out	\$1	\$5	\$11	\$17						
PV of Cash 4 Years Out	\$0	\$0	\$1	\$2						
PV MV + Cash	\$1	\$5	\$12	\$19						
PV Value Per Share	\$0.01	\$0.03	\$0.05	\$0.08						

APPENDIX: PEER ANALYSIS AND SELECTED COMPANY DESCRIPTIONS⁹

Peer Analysis

20-Feb-12

COMPANY	Segment	Ticker	Price	1 yr chg	3 mo chg	TEV	LTM Rev	LTM Growth	Gross Margin	Oper Margin	TEV / Revenue	Emps	Rev / Emp
Symantec Corporation	Security & Storage SW	SYMC	\$17.95	-3%	13%	12,825	6,722	11.1%	85.0%	11.6%	1.9	18,600	361,398
AVG Technologies N.V.	Consumer Security SW	AVG	\$13.52	na	na	1,079	256	0.0%	86.7%	43.0%	4.2	805	317,417
Fortinet Inc.	Security SW	FTNT	\$25.96	25%	10%	3,608	434	33.5%	73.8%	14.4%	8.3	1,527	283,940
Check Point Software	Firewall, Security SW	CHKP	\$58.02	12%	8%	10,685	1,247	13.6%	88.4%	43.6%	8.6	2,239	556,939
Websense, Inc.	Online Security SW	WBSN	\$17.95	-16%	6%	694	364	9.4%	83.6%	8.5%	1.9	1,475	246,904
Tangoe, Inc.	MDM	TNGO	\$17.32	na	26%	544	105	53.3%	52.4%	-2.8%	5.2	873	120,207
Sourcefire, Inc.	CyberSecurity	FIRE	\$35.82	41%	16%	899	150	17.6%	79.5%	4.3%	6.0	351	428,521
KEYW Holdings	Security Services	KEYW	\$7.47	na	2%	244	191	76.5%	29.7%	0.3%	1.3	827	230,456
Imperva Inc.	Online Banking SW	IMPV	\$33.37	na	25%	639	78	41.4%	79.2%	-13.9%	8.2	375	208,805
Bottomline Technologies	Software for Banks	EPAY	\$28.65	30%	35%	907	211	25.6%	54.7%	16.8%	4.3	880	239,352
Vasco	Authentication Security	VDSI	\$10.03	4%	37%	294	168	55.7%	64.3%	14.4%	1.7	353	476,153
Intersections Inc.	Consumer Security Svc	INTX	\$13.12	33%	12%	221	370	2.2%	75.6%	5.5%	0.6	787	470,208
Trend Micro Inc.	Security Software	TSE:4704	\$29.22	-15%	1%	2,536	1,218	1.1%	82.5%	17.3%	2.1	4,846	251,284
Zix Corporation	Secure Email	ZIXI	\$3.21	-18%	21%	190	37	31.7%	80.4%	120.6%	5.1	123	301,667
VirnetX Holding Corp	Secure Communication	VHC	\$24.61	89%	24%	1,178	0	-61.2%	na	na	na	11	2,563
Openwave Systems Inc.	Mobile System SW	OPWV	\$2.52	9%	66%	153	162	-1.7%	59.3%	-18.4%	0.9	536	302,931
Wave Systems Corp.	Security HW	WAVX	\$2.18	-48%	-5%	189	32	32.7%	93.2%	-22.2%	5.9	129	249,161
Average				11.0%	18.7%			20.1%	73.0%	15.2%	4.1		296,936

AVG TECHNOLOGIES (NYSE: AVG)

AVG Technologies N.V. engages in the development and sale of Internet security software and online service solutions under the AVG brand name. Its product portfolio includes Internet security, PC performance optimization, online backup, mobile security, identity protection, and family safety software. The company offers various security suites for core protection, including anti-virus, anti-spyware, anti-rootkit, social networking protection, and LinkScanner; chatting and downloading, such as shield for safe chatting and online shield for safe downloading; shopping and banking comprising identity protection, firewall, and anti-spam; network safety, including intrusion detection; performance, such as system tools, quick tune, and identity alert, as well as suites for expert technical support and to receive priority updates. AVG Technologies N.V. distributes its products to consumer and small business markets online, as well as through a network of resellers and distributors in 185 countries worldwide. The company was founded in 1991 and is headquartered in Amsterdam, the Netherlands.

IMPERVA (NASDAQ: IMPV)

Imperva, Inc., together with its subsidiaries, engages in the development, marketing, sales, service, and support of data security solutions that provide visibility and control over high value business data across critical systems within the data center. It offers SecureSphere Data Security Suite, a solution designed to prioritize and mitigate risks to high-value business data, protect against hackers and malicious insiders, and address and streamline regulatory compliance. The company's SecureSphere is an integrated, modular suite, which offers database security products, which are designed to secure high-value business data in structured repositories in the data center; file security products that are designed to secure files, including spreadsheets, presentation slides, word processing documents, and PDFs containing high-value business data stored by customers in unstructured repositories, such as file servers, network attached storage, and storage area network devices; and Web application firewall product that protects Web applications from large scale cyber attacks and adapts to

⁹ Company descriptions provided by S&P Capital IQ

evolving threats to prevent data breaches. Imperva's solutions secure business data across various systems in data centers, including traditional on-premise data centers, as well as private, public, and hybrid cloud computing environments. Its solutions also include cloud-based security services consisting of Web application firewall services, content delivery optimization, and distributed denial of service-attack prevention that deliver on-demand Web application security. The company provides its products and services to a range of customers worldwide, including banks, retailers, insurers, technology and telecommunication companies, and hospitals, as well as the United States and other national, state, and local government agencies. The company, formerly known as WebCohort Inc., was founded in 2002 and is headquartered in Redwood Shores, California.

VASCO (NASDAQ: VDSI)

VASCO Data Security International, Inc., through its subsidiaries, engages in the design, development, marketing, and support of hardware and software security systems that manage and secure access to information assets worldwide. The company offers hardware and software products in the areas of user authentication, electronic signatures, and digital signatures/public key infrastructure. It provides VACMAN Controller that supports multiple authentication technologies, including passwords, dynamic password technology, electronic signatures, digital signatures, and certificates and biometrics on one platform. The company also offers IDENTIKEY Server, a centralized authentication server that supports the deployment, use, and administration of DIGIPASS user authentication. In addition, it provides aXs GUARD Identifier, a standalone authentication solution, which offers two-factor authentication for remote access to a corporate network or to Web-based in-house business applications; and aXs GUARD Gatekeeper that integrates DIGIPASS to provide secure two factor user authentication. Further, the company offers DIGIPASS product line exists as a family of software and hardware client authentication products and services for authenticating users to any network, including the Internet. Its DIGIPASS solution calculates dynamic signatures and passwords to authenticate users on a computer network and for various other applications. The DIGIPASS technology is also designed to operate on desktop personal computers or laptops, personal digital assistants, mobile phones, and smart cards. VASCO sells its security solutions through its direct sales force, as well as through distributors, resellers, and systems integrators. The company was founded in 1996 and is headquartered in Oakbrook Terrace, Illinois.

INTERSECTIONS (NASDAQ: INTX)

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 credit reports; daily, monthly, and quarterly monitoring of subscriber's credit files; reports and monitoring services based on additional information sources; and credit scores and credit score analysis tools, credit education, identity theft recovery services, identity theft cost reimbursement, and software and other technology tools to protect against identity theft. Its products and services also include consumer discounts on healthcare, home, and auto related expenses; access to professional financial and legal information; and life, accidental death, and disability insurance, as well as distributes online privacy protection software. This segment markets its products and services to credit card, direct deposit, or mortgage issuing financial institutions. The Online Brand Protection segment provides online brand protection services, including online channel monitoring, auction monitoring, and other services to corporate brand owners or law firms, as well as offers forum, blog, and newsgroup monitoring. The Bail Bonds Industry Solutions segment offers 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.

ZIX (NASDAQ: ZIXI)

Zix Corporation provides Internet-based applications in software as a service model that enables the use of secure email for sensitive information exchange primarily in the healthcare, financial services, insurance, and government sectors in the United States. It offers email encryption service, a secure messaging service, which allows an enterprise to use policy-driven rules to determine which emails should be sent securely to comply with regulations or policies. The company also provides a solution that analyzes and encrypts email communications. Its services offer users the ability to deliver encrypted email to any email user at any email address by using the ZixCorp Best Method of Delivery protocol that automatically determines the direct and appropriate means of delivery, based on the sender's and recipient's communications environment and preferences. Zix Corporation sells its services through a direct sales force, and a network of resellers and other distribution partners. The company was formerly known as ZixIt Corporation and changed its name to Zix Corporation in 2002. Zix Corporation was founded in 1983 and is headquartered in Dallas, Texas.

TANGOE (NASDAQ: TNGO)

Tangoe, Inc. provides on-demand communications lifecycle management (CLM) software and related services to enterprises, including large and medium-sized businesses and other organizations. The company's on-demand software and related services enable enterprises to manage and optimize the processes and expenses associated with the lifecycle of an enterprise's fixed and mobile communications assets and services. Its Mobile Device Manager (MDM) application enables businesses to deploy, upgrade, and manage iPhones by providing device and data security, user authorization, cost management, centralized policy control, automated device configuration, application management, self service device deployment, troubleshooting, and asset tracking. The company's solutions also allow enterprises to enforce regulatory requirements and internal policies governing the use of communications assets and services; MobileRenew, a mobile device reuse-retire-recycle program that handles the reuse, retirement, and recycling requirements for various mobile phone and associated accessories; and Tangoe University, a members-only online resource for communications lifecycle management news, expert insight, and information. The company was formerly known as TelecomRFQ, Inc. and changed its name to Tangoe, Inc. in December 2001. Tangoe, Inc. was founded in 2000 and is headquartered in Orange, Connecticut with an additional office in Amsterdam, the Netherlands.

VIRNETX (NYSEAMEX: VHC)

VirnetX Holding Corporation engages in developing and commercializing software and technology solutions for securing real-time communications over the Internet. Its software and technology solutions, which include secure domain name registry and GABRIEL Connection Technology, facilitate secure communications and create a secure environment for real-time communication applications, such as instant messaging, voice over Internet protocol, smart phones, eReaders, and video conferencing. The company focuses on commercializing its technology to original equipment manufacturers within the IP-telephony, mobility, fixed-mobile convergence, and unified communications markets. VirnetX Holding Corporation was founded in 2005 and is headquartered in Scotts Valley, California.

OPENWAVE (NASDAQ: OPWV)

Openwave Systems Inc. provides software solutions for the communications and media industries in North America, Latin America, Europe, Africa, the Middle East, and the Asia-Pacific. Its product portfolio consists of server software products, which include mediation and messaging application products for mobile operators. The company's mediation software products comprise all-IP Openwave Integra platform to help mobile operators for capturing a share of the mobile content market; Openwave Passport Smart Policy; Openwave Media Optimizer, a callable and policy-aware video delivery solution; and Openwave Web Optimizer, a Web caching and compression solution. Its messaging products include Openwave Email Mx, which delivers carrier-class messaging to serve wireline, wireless, and ISP customers; Openwave Rich Mail, a PC-based Web 2.0 solution that enables broadband and mobile operators to brand, personalize, and monetize messaging offerings; Openwave Smart User Repository, a user data storage solution; and Openwave Multimedia Messaging

Services Center, which enables operators to offer multimedia services, such as integrated photo and text messaging. In addition, the company offers professional services, and maintenance and support services. It sells its products and services through direct sales force and third-party resellers. The company was founded in 1994 and is headquartered in Redwood City, California.

SOURCEFIRE (NASDAQ: FIRE)

Sourcefire, Inc. provides intelligent Cybersecurity solutions for information technology (IT); environments of commercial enterprises, such as healthcare, financial services, manufacturing, energy, education, retail, and telecommunications; and federal, state, and international government organizations worldwide. Its Sourcefire 3D System comprising multiple Sourcefire hardware and software product offerings provides an approach to network protection with a layered security defense, protecting computer network assets before, during, and after an attack. The company also offers Snort, an open source intrusion prevention technology that is incorporated into the intrusion prevention system software component of the Sourcefire 3D System; and ClamAV, an open source anti-virus and anti-malware project. In addition, it provides various services to aid customers with installing and supporting Cybersecurity solutions, including customer support, education, professional services, the Sourcefire vulnerability research team, and Snort rule subscriptions. The company has strategic relationships with various managed security service providers, including BT Counterpane, SecureWorks, Symantec, VeriSign, and Verizon Business to provide alternative distribution channels for its products. Sourcefire, Inc. was founded in 2001 and is headquartered in Columbia, Maryland.

DISCLOSURES

StrikeForce is a research advisory client of Research 2.0. We have provided independent analysis, conducted our own due diligence, built our own financial model and valuation and given the company our best ideas surrounding investor positioning. In exchange for these services we have received compensation (not in form of warrants, options or restricted stock). We also publish the results of our work for informational use. We maintain our own independent research process, exercise full editorial control of all published content and apply the same standards to advisory clients as we do to all companies we follow. Research 2.0 employees are governed by rules to ensure that the interests of the organization are aligned with those of clients and investors. For additional information about our services, disclosures, disclaimers and employee policies, please visit our website.