CEO CFO

StrikeForce Technologies, Inc.

Issue:
February 11, 2011

The Most Powerful Name In Corporate News and Information

Given the Rise in Identity Theft and the Use of Mobile Devices, StrikeForce Technologies, Inc. is in The Right Space at The Right Time with their Patented Out-of-Band Authentication ProtectID® and Keystroke Encryption GuardedID®

Technology
Business Security Software
(SFOR-OTC: BB)

StrikeForce Technologies, Inc.

1090 King Georges Post Road,
Suite 603
Edison, NJ 08837
Phone: 732-661-9641

Mark L. Kay
Chairman and CEO

BIO:
Mr. Kay joined StrikeForce in May 2003 as the CEO. The public Company developed proprietary software that "Specializes in Preventing Identity Theft." From August 1977 through December 2002, Mr. Kay worked at JPMorganChase & Co., where, for the majority of his 26 year employment he was a Managing Director. During his employment at JPMorganChase & Co. Mr. Kay globally led strategic and corporate business groups. His responsibilities included Chief Operating Officer, Chief Information Officer and Global Technology Auditor during his tenure mostly relating to the Investment and Securities Divisions along and Audit. Prior to his employment with JPMorganChase & Co., Mr. Kay was a Systems Engineer at Electronic Data Services (EDS) for over five years. He holds a B.A. in Mathematics from CUNY. Mark is on several university business and computer science advisory boards.

Company Profile:
StrikeForce Technologies helps to prevent identity theft online. Its products help protect consumers and their families while banking and shopping online, enterprises and government agencies in "real time" against data loss and data breaches. StrikeForce Technologies, Inc. (OTC.BB:SFOR) is headquartered in Edison, N.J.

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFOinterviews.com

CEOCFO: Mr. Kay, what role does StrikeForce play in identity theft protection?
Mr. Kay: It is a very exciting time these days because, we all know Identity Theft has taken off in leaps and bounds. There are billions of dollars being lost yearly and our two products are smack in the middle being able to solve some of the core problems that are going on. We have two major products that we will talk about, ProtectID® and GuardedID®. ProtectID is our two-factor Out-of-Band Authentication product that is now patent published as of two days ago. ProtectID plays a major role in allowing banks to authenticate customers and employees signing into their network in the strongest ways possible. It has been written up by Gartner, Forrester and others that by using various Out of Band methods is recommended in preventing identity theft. Our GuardedID® product is a keystroke encryption product that prevents malware from stealing keystrokes, which has become the number-one reason for data breaches occurring around the world. That is one of the only products, unlike the anti-virus programs that don't prevent data breaches from occurring real time. Both of our products have been out there for a few years, which have been greatly enhanced. Now that the market is finally catching up to our solutions, realizing the problems of identity theft is increasing exponentially SFT is gaining increased market acceptance and traction. Identity theft is now affecting every consumer, every employee, and every company to some extent.

CEOCFO: Would you explain the two-step authentication?
Mr. Kay: The majority of people when they bank today online or go online to do transactions over the Internet, are still using a username and password. Some use picture IDs and a few use a phone call; they get the phone call back and they get a password or pin and they enter it in the computer or the other way around. However, the username and password no longer protects anybody from anything. In addition, the regulations now, which primarily include the FFIEC and Red Flags and HIPPA for starters, are requiring the financial industry and all industries when processing any trans-

actions relating to personal information or money or consumer private information through the internet, must offer two-factor authentication solutions. As written by various analysts, they strongly recommend using Out-of-Band methods of authentication as the strongest. What does that mean? Two-factor authentication is something you have and something you know. Something you have does not count as a computer. Something you have would be a phone, some device, a token or something that is outside the computer, so not to be seen or stolen by a thief who is stealing through the internet or has malware on your computer. The Out-of-Band process talks about sending your personal pin or password through a second channel, like a phone. Your one-time password is typically used where the numbers keep changing, so you don't have to memorize a pin, then sent or received through another channel other than the internet, which typically is a telecommunications channel. For instance with some banks now, especially one of our biggest clients, one of the major investment banks on Wall Street, you log into your system, you put in your username into the computer, your phone rings, it asks you for your one-time password. You get the one-time password on the computer from the bank, you enter it into the phone and you then complete your logon or transaction. Your one-time password was entered into your phone, not into your computer, so it can't be stolen or combined with your username through the Internet. That is much stronger than just a hard token, which we also offer on our platform. Many companies like PayPal offer these hard tokens with numbers that keep changing, which that is still two-factor, because it's something you have and something you know. Something you have is the token, but it is not Out-of-Band because it is all being done through the computer through the internet, so that is not as strong. More and more banks are requiring an Out-of-Band method for high risk transactions including money movement. When it comes to Out-of-Band methods, our ProtectID product that is registered and now patented is the only one of its kind that offers the most methods of authenticating a person or an employee at the same time with the greatest depth in terms of opportunities of adding new methods and working in all technology environments. That product is offered by us as a cloud service, but it also can be installed locally depending on the preference of the client. Our two major competitors in the Out-of-Band communication space only provide a service, and some of the major companies that we know out there like the Vasco's and RSA's that are well known for their authentication hard and one time password soft tokens products, do not offer Out-of-Band authentication. Therefore, we are in a space that is quite limited in competition which is now becoming one of the most critical things that the major financial and soon healthcare with their regulations, and government is adopting. Because people are moving away from the hard expensive tokens that people lose and batteries die, to an Out-of-Band method. It could be phones, or anything that you already have with you that does not add cost.

StrikeForce definitely is a company that has two major products that prevent identity theft that have become two of the hottest issues today. What hasn't allowed us to move forward in the past is the markets were not ready, the regulations were not strong and we lacked investments. All these things now have turned around. The markets are hot, the regulations are strong, the investors we have are tremendously connected. They are reaching out in many directions. - Mark L. Kay

CEOCFO: Is the consumer ready to make the trade-off between security and extra steps to be secure?

Mr. Kay: That is why we are now starting to see success and why we didn't see success seven years ago and not ten years when we invented the Out-of-Band process. Because it was deemed to be too difficult, too much extra work, not user friendly. What is happening now is the media is helping tremendously. There is almost a news article everyday about identities being stolen, about monies being stolen out of banks online. If you like username and password and don't want to do anything else, beware that when your identity gets stolen, and the bank may not be fully responsible if it is not reported within 30 days typically or caused by malware on your computer, which is typical; and it will take up to three years to get your credit back in either way. Or you can deal with getting a phone call and on your computer you get something back from the bank that gives you your one-time password and answering the phone and putting the one time password into the phone, which takes seconds to do, which pretty much guarantees that your identity won't be stolen. In this process, now the bank is responsible because they are offering the method and they are responsible and more likely you won't experience identity theft. That acceptance level has gone up tremendously lately, because of the media and because of the issues around data breeches, as well as the inconveniencing of individuals being more acceptable, let alone less monies lost. It is changing and that is why we are starting to be more successful and the regulations are requiring the companies to increase authentication as well. Therefore, they are requiring consumers to accept the extra step and of course they don't charge them for that added protection, which is why we need a lot of volume to make major revenues. However, it is moving in the right direction for all the right reasons, including with the increased revenues.

CEOCFO: Are the bigger banks taking the lead on increased security or are the smaller banks adopting more quickly?

Mr. Kay: It is both, but when you think about the bigger banks, they run their own systems and processes. We are working with one of the largest firms on Wall Street and their audit department says they now have to add Out-of-Band authentication, not just two factor. Tokens are not good enough and user name and password

is definitely not good enough. They have to add Out-of-Band in order to allow people to process money movements through their company. People do like the convenience of doing a wire transfer on a computer and not having it go to the physical bank. To do that they must use a product like ProtectID and the more people start to use it the more they will get used to it. It is no more difficult than answering a phone call and typing five or six digits on it, and knowing that that secures you more than the other methods. People are feeling much better about that. When I say phone calls, it is not just cell phones. However, everyone walks everywhere with a cell phone these days and therefore the inconvenience of getting a phone call on your cell phone is not an inconvenience in this day and age, which is why it has become much more acceptable. Text messaging is another way of completing an Out-of-Band authentication, which isn't as secure, yet we are seeing the text messaging is now up to about 45%, because people have choices when they use our product and go for simplicity. We are seeing strong movement toward Out-of-Band and being more acceptable by all.

When it comes to Out-of-Band methods, our ProtectID product that is registered and now patented is the only one of its kind that offers the most methods of authenticating a person or an employee at the same time with the greatest depth in terms of opportunities of adding new methods and working in all technology environments. That product is offered by us as a cloud service, but it also can be installed locally depending on the preference of the client. - Mark L. Kay

CEOCFO: Would you tell me about the keystroke protection product?

Mr. Kay: The competition is not the major companies you would expect; they do not provide keystroke encryption. It is a couple of other small companies in our space that primarily provide banking technology. The media has published articles out being clear about the risks of keylogging and data breaches. On the GuardedID side, that is a product we developed six years ago and in concept seven years ago, completed three years ago and just now starting to have some major sales this year, because it is another product like antivirus programs. Everybody has an antivirus program on their computer whether it be Norton, or Mcafee as examples, but most people don't understand they do not prevent malware from stealing keystrokes real-time. This is because the way they work, they have to find out what the malware looks like, which is a program in your computer. You cannot prevent this type of malware from getting into your computer. These antivirus programs approximately 90% do not prevent keylogging, and especially when they happen real-time (zero day); not until the anti-virus products figure out what the malware looks like, do they sometimes give you an update to knock it out many days later. Meanwhile, every keystroke you type on that keyboard, your name, social security number, or password; even if they are complicated passwords, are stolen. They are stealing what is in the computer and it doesn't matter what data is in the password field, however complicated it is. So it is the most dangerous fate. The 2010 Verizon Data Breach Report talks about malware stealing keystrokes, known as keyloggers, as the number one data theft occurring. These are most or all of the major data breaches. We have all heard about Heartland Payment Systems, TJ Max, and others, which were stolen through keyloggers, getting into computers and stealing critical data such as usernames and passwords. If you had ProtectID then the keyloggers wouldn't matter, because they would not be able to steal your password that goes through an Out-of-Band method, but if you do not, it will steal the passwords and other information. We have the only program out there that prevents the keyloggers from getting your keystrokes real-time, not only when you are working online, which two of our competitors do, but also when you are working offline on your computer. If malware is in your computer, as it typically always is, whether you are online or offline, it is stealing your keystrokes and when you are online, it sends it to the bad guys. With us, we are active all the time, even when you are working in the Microsoft suite of Word, or Excel; any application in your computer at anytime whether you are online or not, you will be protected through our GuardedID program. This is becoming a very hot issue. Our clientTrend Microannounced publicly almost a year ago the inclusion of our product, GuardedID. Trend Microis the only antivirus program that included an anti-keylogger as strong as ours. They sell it and push it out globally through their product because they know they do not prevent keylogging otherwise; none of them do. We have many other clients implementing GuardedID. We will be announcing in another month a major ISP telecommunications company in the United States; one of the largest ones there are and our product will be included in their offering. We are seeing major interest with that product because malware is increasing greatly. It is becoming the biggest issue for identity theft and malware stealing keystrokes is the biggest issue. By the way, the malware gets into a computer and isn't stopped by your firewall. It gets in through emails, pictures, and through songs. It can get into your computer every time you stick something into a USB port, whether it is an electronic picture frame, or anything you ever buy or an mp3. Whatever it is, you have no way of knowing if it includes malware that steals keystrokes that slithers itself in the computer like a worm and you will never know it is there.

CEOCFO: Is this GuardedID only being offered through other programs, or is it something you are offering direct to consumers?

Mr. Kay: If you went to our site www.guardedid.com you can actually buy it. It is $29.99 right now for one-year subscription and get automatic renewals of $24.99 every year thereafter. So it is sold direct to consumers through us. We have many affiliates who sell it direct to consumers or indi-

rectly through bundles. If you have Trend Micro you can go to the Trend Micro free store and pick up a GuardedID copy there as long as you continue to use Trend Micro. Another client, Identity Guard is a major program that many people hear about all the time through adds. Intersections, the company advertises that it if your identity gets stolen, if you buy their premium version, it includes a product called Privacy Protect. That is GuardedID in a private label. Therefore, we are showing up in many flavors and many places. You can go to our website directly and buy it yourself now and protect yourself.

CEOCFO: Sometimes antivirus programs block things you do not want to block; is GuardedID basically seamless?

Mr. Kay: That is a great question, and in the beginning yes. In the beginning, we ran into other programs that didn't play nicely with us. Not everybody follows the Windows process in every which way. The good news is we have gotten past 99.9% of those issues. The reason I say it that way is I have been in this business for 40 to 50 years in technology and there is no such thing as 100%. Every once in a while somebody is going to find something that might cause an issue. Typically, the only issue will be the green we show in the field you are about to type in will not show up. Our online product is in the toolbar and when you type on a field in Internet Explorer or FireFox, your field turns green so you know it is clean and safe, and then you type; you know a keylogger can't get it. We have hundreds of thousands of licenses out there and we get maybe, maximum, a call a day that we have to deal with, so that is a way of us understanding it is working with 99.99% success with everything out there. Plus, when we went with Trend Micro, we had to build it it in fourteen languages. It is running all over the world on their programs including Asia, which is the most difficult with the double-byte languages. It is going very well. With new clients we are bringing on board we will be in the tens plus millions more copies being distributed over the coming year, so we feel excellent with the progress and market acceptance. Put it this way, we know it is stronger than Microsoft's products, but that does not necessarily say a lot. This only works on Windows platforms, we do not have the Apple version yet, but we are working on that.

CEOCFO: What is the financial picture like for StrikeForce Technologies today?

Mr. Kay: We are seeing 2011 as an incredible year for us. We had an amazing 8K announcement about a month ago where we received funding from an investor group. We talked about it being close to $1 million. They bought out the prior secured lender, which was Yorkville Advisors, so we are dealing with an extremely friendly company who also announced bringing in an approved government contractor for us to work with and distribute through. This would be a multimillion dollar revenue based approved government contractor with major clients like Boeing, Lockheed and others. They we are now a part of the whole process and we can put contracts through them as appropriate. It is incredible business that what we have lined up. We are excited as can be; especially getting the patent two days ago being published for Out-of-Band Authentication. Just imagine that. You have many companies out there using Out-of-Band processing that roll their own that we now have the patent for, so it is a huge opportunity in itself. We are very excited and we see some large increase in revenues. People have seen a 1000% increase in our stock price by bringing in this new secured lender, versus the one that was there before. It is major progress, so we are very excited. In addition, we will be at the RSA show at booth #2117, which is a sizeable booth right up front near Microsoft, and Symantec. It makes it a big splash and a big statement.

CEOCFO: Do you do much investor outreach?

Mr. Kay: We do, and we provide it through a group we have on board now, but we have been doing a lot more of it lately leveraging various avenues.

CEOCFO: In closing, why should potential investors choose StrikeForce?

|**Mr. Kay:** StrikeForce definitely is a company that has two major products that prevent identity theft that have become two of the hottest issues today. What hasn't allowed us to move forward in the past is the markets were not ready, the regulations were not strong and we lacked investments. All these things now have turned around. The markets are hot, the regulations are strong, the investors we have are tremendously connected. They are reaching out in many directions. We already have a stock price increase of over 1000% since they started about a month ago and we have more clients now interested in the company. We have a company we can put our contracts through, if they prefer a stronger balance sheet, so there is no one that we would not be able to bring on and do business with. We have strong resellers now that are more interested and the more we move forward the easier it gets to bring on additional clients. We see huge jumps in revenues this year and we do expect to be cash flow positive around mid-year based on contracts already in place that I could not mention at this time.