CEOCFO Magazine

ceocfointerviews.com

Issue: September 11, 2017

Q&A with Greg Wolfond, CEO of SecureKey Technologies Inc. Increasing Security of Online Transactions, Services and Applications using Facial Recognition Software to provide a Frictionless Digital Identity

Greg Wolfond
Chief Executive Officer

SecureKey Technologies Inc.
www.securekey.com

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

"The ecosystem is all about empowering the consumer to be able to have access to their data and share it where they want to."- Greg Wolfond

CEOCFO: ***Mr. Wolfond, the first thing I see on the SecureKey site is "An ecosystem approach to frictionless digital identity. What is SecureKey?***
Mr. Wolfond: We are generally big believers that it is too hard for all of us citizens and people to get things done online, to prove who we are and to get access to the services we need. We show up at a call center and have to prove who we are, and answer questions that we may or may not know the answers to, restricting us from proving that we are who we say we are to open a bank account or access government services. That is some of the friction that we talk about that can be expensive and is painful for consumers. To resolve this, we are trying to bring together an ecosystem of banks, telcos and governments to work together to make it easier for people to prove who they say they are and get access to critical services, such as call centers, online or in person.

CEOCFO: ***Are we talking about a universal password? How are you achieving the goal?***
Mr. Wolfond: It is a lofty goal. The challenges of cyber is out there everywhere and the bad guys have accessed 3.4 billion records so far in 2017. They know the answers to the knowledge-based questions better than the consumer does. They are able to copy a driver's license with accuracy. In reality, for businesses and government, it is hard to know whether to trust if a person is who they say they are. Our belief is if we can combine the strength of logging into your bank right now and proving that transaction is coming from your mobile phone we can increase the security of that transaction. If additionally we can verify, always with with consent, the location of the mobile device and even validate your face against the provincial database or state database this will increase security The combination of those things together – where I can know it is coming from a device, I know you know your password and I know I can check your face against the state – will improve security. If you put those together, of what I know, what I have and what I am, you can decrease the risk of an impersonation and you can reduce the friction so consumers can show up and prove who they are in seconds, instead of lining up in an office or bank branch for three minutes just to open an account.

CEOCFO: ***How are you able to read a face that it is going to match for most people even if they did not look the same as they did six months ago?***
Mr. Wolfond: The technology is getting much better at detecting a live person. Is it actually the person they say they are? It is the combination of various methods of identification that is most important: being able to do a facial check and say "yeah, that is basically Greg," logging into Bank of America and prove he knows the password and he can prove he has this phone from Verizon. When you take the factors together, you get to a really strong level of assurance that it is actually Greg applying for that service. The biggest point here is that one party by itself cannot solve this problem. Banks cannot solve it on their own with things like user ID, password and knowledge-based questions. The telcos cannot solve it just because they know the SIM is in the device and location of device. Governments cannot solve it because they do not have passwords and do not remember the infrequently used passwords and things for government. Our belief is if you can put all those working together in a model where the consumer is in charge to choose to share their data. If consumers have trust in security, then they will use these services because it gives them more access and safety in going online and going to places on the phone.

CEOCFO: ***I am guessing that most consumers are not reluctant to share their data if it is makes for easier process or do you find some, like me, who are more skeptical?***
Mr. Wolfond: We are already sharing it today. We show up at a telco branch or bank branch and we want to prove who we are, so we show a driver's license or passport, as well as a copy of the statement or bill. All this stuff exists today. You have to prove who you are and you bring in artifacts with you. Very often you do not have the right things with you – when you are getting an apartment, the landlord wants to know if you are who you say you are, prove to them that your credit scores are over 650, and they want a background check to make sure you are not a violent offender. To go get all of the information and prove your income can take days or weeks. What if you could just show up and with your consent – you agree to share your name and address, your bank information, your credit score from Equifax or TransUnion, your background check – and just provide it to a landlord so you can rent an apartment right now. That makes a huge difference for you.

Our model really focuses on this privacy by design, where only the consumer can consent that they agree to share this data with this party for this purpose. That is what is exciting for state government, banks and telcos, because this is your data to use and only you should be able to say yes you agree to share these parts with this party. We do it today in the manual world but how do you bring that to that electronic world and how do you do so with privacy?

When we talk about some of the sharing, it is not hard to do electronically, but you have to mimic some of the things that work in the manual world today. For example, when you show your driver's license at a bar or liquor store, the state cannot know you went to a bar or liquor store. Today it is a physical piece of plastic, so there is no way to know where you have used it, but the bar and the liquor store trust it. In the world that we are building, we are looking to implement those same characteristics.

CEOCFO: ***Who is using your services today?***
Mr. Wolfond: The first service that we launched in Canada was for authentication, for consumers looking to show up at a government website and log into CRA – the equivalent of the IRS in the US – or other unemployment, benefits or immigration departments, among others. Instead of having to create a different user ID and password, each department, and then forget that next year when I come back, I instead can choose a bank I want to log in with like TD Bank or Royal Bank to access the service. I do not have to create new user IDs and passwords. On our platform, we have about eight million credentials registered in Canada and had about 300,000 users every month. It is active and in use.

CEOCFO: ***What about the US market?***
Mr. Wolfond: We are just getting ready to launch to the US. We are in dialogue now with telcos, banks and governments and they are very keen on this model because it meets the requirements that are set up by the National Institute of Standard and Technology (NIST). They set new guidelines, the 800-63 guidelines, that said it is really important to allow people to share data and information about themselves, but also very important that privacy is there and that nobody should be able to track where you are going. Our platform is one of the only systems that meets those new criteria that are coming out now. We are strong enough that just in the last few months, we received a grant from homeland security saying this is the way people can share their information with privacy and security. We will launch very soon in the US.

CEOCFO: ***Would you tell us about the blockchain approach and what people should understand?***
Mr. Wolfond: Blockchain is a complicated topic. There is a difference between our technology and Bitcoin, which is a payment system and the underlining blockchain technology. We are not developing a payment system, but we are using some of the principles of the underlining technology. The most important of those is that we needed different ledgers and trusted places to make sure we had those privacy characteristics that when you share your data, there is no way that the provider of the data knows where you are sharing it, there is no way the network in the middle can ever see the data in transit or at rest and the receiving party should not necessarily know who the provider is. For example, if I am sharing information from TD Bank, I do not need the service I am sharing the information with to know I bank there. We call this triple blind. We could not develop triple-blind architecture for sharing data unless we had this distributed ledger architecture underneath, which is blockchain.

The other thing we get for having blockchain is resilience. Today when we build systems, we have a big server in the middle and you can get a denial of service attack from baby monitors or bad devices out there, which can take down the whole service. We cannot have a service that is susceptible to denial of service attacks. We needed something that is resilient. In Canada for example, in order to take the network down, you have to take down Royal Bank, TD Bank, ScotiaBank, Bank of Montreal, etc.,and all the other parties running the nodes. That is the beautiful thing about this architecture – it has resilience against denial of service attack.

CEOCFO: ***What is the business model?***
Mr. Wolfond: It is absolutely free to consumers. It is a value-added service for consumers. It is provided by their telcos, their banks and their

province or state. When the consumer elects to share their data, we have to record that they consented to share this data with this party at this time, and we are able to deliver the data to the party that is requesting it. The party that is requesting it – whether a bank, telco or government – wants to know it is really who they say they are. They are willing to pay a small fee for the bank to confirm "yes, that is Lynn" and are they logged in right now as Lynn. The telco will say "yes, that transaction is coming from her phone." Depending on the service you are accessing, they are going to want more or less security. If they want more, they can pay for more data and if they want less, they'll pay for less, but the goal is to keep it inexpensive and keep it super secure and private.

CEOCFO: ***What is involved in implementation?***
Mr. Wolfond: The beauty of what we have built is to implement this at a state, it is really a very standard OPEN ID and OAUTH connection. One of the provinces we connected into the network took three days. They do not have to get into the depths of blockchain or how it all works; we make it very simple on the connection end to make sure they know they have security and they can share their data with trust.

CEOCFO: ***When you are approaching an organization, is there an aha moment when they understand and does it matter who you are speaking with as to whether they will recognize the concept?***
Mr. Wolfond: It seems to be pretty broad. All of the organizations we speak to – across government, banks, telcos or healthcare – have as one of their first, second or third priorities right now to become more digital and more cyber secure. If you want to become more digital, you have to be able to serve customers who show up digitally. The ability to let the customer prove who they are to get through the KYC (Know Your Client) or AML (Anti-Money Laundering) process to prove that they are them to open an account has to be simpler than it is today and it has to be more secure.

All of these organizations recognize today that there are holes. Hackers are gathering data and answering the knowledge-based questions to prove they are Greg when they are not Greg, or they can show up with a document and driver's that say that Greg is not really Greg. They are trying to raise this security bar and make it harder for the bad guys to act as you, but easier for you to be you. They realize that by combining telcos, banks and states, we can actually get a solution that works for real people that lowers the cost overall, making digital happen much faster and makes the fraud go right down.

CEOCFO: ***Would credit card companies be able to embrace this as well?***
Mr. Wolfond: A lot of the credit card companies use knowledge-based questions, yet over 30 percent of customers cannot answer the knowledge-based questions. Banks need to know it is really you so they can give you a credit card that has a reasonable credit limit. By investing in a more secure online platform, like the one we are building, if consumers are requesting a credit card, they could adjudicate and issue that card much faster than they can today with much more security.

CEOCFO: ***What has changed in your approach as people have started to use SecureKey's offerings?***
Mr. Wolfond: We are learning it is a lot more than just identity. There is data that is in different places that people want to share. Healthcare is a

great example. I have health records at my own doctor and health records elsewhere, and each one has its own user ID and password. The combination of all that makes it impossible for me to remember all of my passwords and log in credentials, but what if I could use a system to show up, put my finger on my iPhone and prove who I am to each of these organizations? Then I could see all my health records. If I decide to share my health records from one provider to another, I should be able to consent to show those records and they should be sent – as opposed to coming into the doctor's office to prove who I am, having them fax my data a week or two later to the doctor I am trying to go see for a problem I want to get dealt with now.

We started the service with identity and we are learning it is a lot more than identity. It has massive implications to healthcare - you consent to share your data for clinical trials where we could save billions of dollars in cost. There are massive implications for getting a mortgage, when we can prove from the government your income for the last three years and prove your credit from a credit agency. All that can be compiled into one place with consent, so that process now takes a fraction of the time.

CEOCFO: ***With so much potential or opportunity, how do you come up with a longer term strategy and decide where to focus your efforts?***
Mr. Wolfond: We are pretty good on focusing on where we are. We started in Canada and they are seeing huge adoption across provinces, banks, telcos and organizations who want to build applications on top, and now we are picking the markets to come next. The US is clearly on that list next. In line is a couple other markets we are going to launch as well.

This offers so much value to the telco, to the bank and to the users of the service who in many cases want to be able to provide data for their customers, but they also want to receive data from others to make their processes better and more efficient. It becomes this ecosystem that we talk about on our home page. Without the ecosystem, if I am just providing data, it does not do a lot. If it is a bank only thing or a telco only thing, it is never going to scale to the level it has to scale. The ecosystem is all about empowering the consumer to be able to have access to their data and share it where they want to. Consumers want to be able to access and use their data at the ready, whether it is to healthcare services, accessing a bar, or creating a new government, I can prove who I am and not get stuck on a call center call, being asked questions that I cannot answer. My time is going to be better spent as a consumer and the harder I make it for the bad guy to impersonate me, the better it is going to be for everyone.

CEOCFO: ***Do you help an organization provide information to their customers about how to use SecureKey and do they use the SecureKey name?***
Mr. Wolfond: In some cases, it does not really have to be about SecureKey. It is very much about our partners and their customers. The whole notion is that we are a connector brand. It is not supposed to take away from their brand, but it helps their customers know they are dealing with a trusted service.

CEOCFO: ***Why is SecureKey an important company? Why pay attention right now?***

Mr. Wolfond: People do not really know yet what digital identity is, but they know when they show up at a call center, or online or in person to prove who they are, it is riddled with friction, is hard and the bad guys are getting through. If we can find a way for consumers to share their data to prove who they are and get services in a fraction of the time with more security and privacy, then consumers will be happy. We expect to see similar results to what we found with our Concierge service in Canada, that consumers kind of flock to the surface because it is a need that is not being met today.

CEOCFO: ***Final thoughts?***
Mr. Wolfond: Cyber fraud is a reality and is rising. We think there is real need to allow people to prove who they are and make it harder for bad people to prove they are consumers. Without bringing together this ecosystem of banks, telcos and government, we are not fully going to address the problem and we are not going to make it better for people and organizations.