ceocfointerviews.com

Issue: December 4, 2017

CEOCFO Magazine

Q&A with Bob Geiman, CEO of Confirm.io using AI, Computer Vision and Machine Learning to provide Mobile ID Digitally Authenticating with their Solution now in many Large Banks, Insurance Companies and Hospitals across the US

Bob Geiman
CEO

Confirm.io
www.confirm.io

Contact:
J. Robert Geiman
617-513-9145
bgeiman@confirm.io

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

CEOCFO: ***Mr. Geiman, we spoke about eighteen months ago when Confirm was a relatively new company. Today I see you are helping over 850 organizations authenticate customer identity documents from around the world. Would you bring us up to date?***

Mr. Geiman: A couple of developments have occurred in the marketplace that have really accelerated interest in and adoption of our technology. First, earlier this year, NIST (National Institute of Standards and Technology), which is a subsidiary of the Department of Commerce, published guidelines declaring that biometric authentication on its own is not enough to authenticate identity—biometric authentication must be paired with another authentication method. NIST also cautioned on solely relying on more traditional identity authentication services that are based on information you know like social security numbers, passwords, mothers' maiden names, etc. These data sources have been compromised by the growing number of cyber security data breaches. Fundamentally, there are three basic ways to assert that you are who you say you are: something you know (like a password or social security number), something you are (biometrics) and something you have (like a government issued document). So, in a world where NIST recommends multi-factor identity authentication, meaning relying on more than one paradigm, and has recommended moving away from using a paradigm based on something you know, the options are biometrics and something you have—Confirm focuses on the later where our authentication methodology is based on digitally authenticating any government issued document. Historically, these NIST guidelines aren't mainstream and are generally read by security professionals. What has become mainstream is a growing consumer awareness of the dangers posed by large scale data breaches like we just had with Equifax. Consumers definitely have a greater awareness of the dangers of identity authentications based on social security numbers, mother's maiden names and passwords because the average consumer now knows that anytime you store data, that data has a high likelihood of being compromised at some point. These traditional authentication mechanisms also create liability for the corporations and the executives that use them. These market developments have placed a lot of attention on ways of authenticating identity like our products, and are the reason why we have large partnerships with organization such as Experian, iPipeline, and Neustar. In the past 9 months alone, we have closed business with over thirty companies that are using our mobile solution, replacing or augmenting some of those more traditional services. We are in trials with most of the large banks in the United States and a number of large insurance companies. We are about to close a significant partnership with a company that services over 60% of US hospitals, so we have had a tremendous amount of commercial traction this year due to these favorable market developments.

CEOCFO: ***Why are these organizations confident in the Confirm solution?***
Mr. Geiman: Our solution is based on authenticating a government issued document. Some of the confidence level stems from the confidence that organizations and individuals have in government issued documents and the process that people have to go through to get a government issued document—an in-person identity proofing process coupled with a lot of supporting documentation. A lot of what we are doing is extending that process to the digital world, and creating a frictionless digital authentication paradigm that relies on a document that can only be issued after an extensive process—increasing the confidence in a digital authentication process that relies on this document. Confidence in Confirm.io has also grown because we have been able to close business with large enterprises and channel partners whose technical diligence process is both respected and trusted. Just being in a market with real referenceable customers always helps. Thirdly, our customers have, in many ways, had no choice but to look for other mechanisms like Confirm to authenticate identity that are different than the traditional methods because the growing threat of cyber security data breaches have put a lot of pressure on customers to change their business processes.

CEOCFO: ***What is involved with implementation?***
Mr. Geiman: It is actually fairly simple. We are an API driven company so, for some customers, deployment of our technology is as simple as doing an API integration and that can take a day and a half of engineering work. It is fairly simple. The alternative is to embed our SDK into a mobile application—also a fairly simply process. Finally, we can quickly port our backend into a customer's cloud or datacenter—we just had a large financial services company port our solution, with our help, in two days. Customers certainly have to change their web and mobile user experience. Instead of asking questions like what is your password or social security number, customers need to build digital experiences that enable the capture of a government issued document using their mobile phone.

CEOCFO: ***What is the process?***
Mr. Geiman: Our customer has a choice of how much friction / authentication they want to introduce and at what point in their consumer experience workflow a customer wants to introduce that friction. A full authentication through Confirm.io requires a consumer to take a picture of both sides of a driver's license or one side of a passport, and then a selfie whose image we can compare against the picture on the government issued document. We use artificial intelligence, computer vision and machine learning technologies to authenticate that the document is real and then we match the selfie to the picture on the document to confirm that the person who is holding the document is the same person whose picture is on the document. That is the full process but the reality is that a customer can decouple those steps and implement different steps at different times in the consumer lifecycle. As an example, we have a large credit card issuer who uses back of the ID authentication only at initial onboarding—a product we call Instant Verify. On their web portal for a credit card application, the customer initially asks a consumer for their name and phone number. This generates a text message. The consumer clicks on the link embedded in the text message—this launches our product where the consumer is instructed to take a picture of the back of the ID only. Our product will then route the consumer back to the website and fast form fill all the data from the barcode on the document to relieve the consumer of needing to enter that information. In under 3 seconds, Confirm then authenticates the back of the document and automates the collection of that document for our customer. The consumer can then press click to get approved for a credit card. If the same consumer wants to get a higher credit limit or transact for the first time, this credit card issuer will have its consumers at a later date, after the card has been shipped, take a picture of the front of the document, the back of the document and then a selfie—for a richer, more secure authentication process. What we have discovered this year is that there are two constituents inside companies that make a decision around remote identity proofing and digital consumer enrollment. Certainly, the security and fraud team needs to meet their authentication requirements. But Confirm also needs to sell the consumer experience / e-commerce teams who need to manage how much friction / authentication they put in front of a consumer and at one point of the customer lifecycle they introduce this friction. As an example, if this credit card issuer asked its consumers to do our full authentication process before that consumer was initially issued a card, our customer would experience some greater drop-off—abandonment in e-commerce parlance. Therefore, instead this customer requires back of ID authentication only at the time of issuance and ask its consumers to do a full authentication only after a card is in the consumer's possession. At that point, there is a belief that a consumer will be willing to do more to get more credit or to use the card. That has been a big driver for us--our ability through the componentization of our product to enable our customers to balance their consumer experience with security and authentication.

CEOCFO: ***Can you guide a company in how to use your solution?***
Mr. Geiman: Ultimately, it is up to them but we do have a number of customers whose experiences and implementations can help our future customers. We also have a number of different demos to show how you can mix and match our technology to achieve a desired workflow. The reality is most of our digital customers are trying to manage two separate and distinct problems: the cost of acquisition and the cost of fraud. For the people on the e-commerce side of the house,

these people know statistically that, when they force a consumer do one more step, there will be some percentage drop-off. The question ultimately is what is the right mix between friction / authentication and an elegant consumer experience. Our customers will implement our best practices, trial various demos, do A/B testing—in an attempt to answer that question. These customers will also look at some of their past consumer workflow / digital experiences to inform the decision about how much friction they can put on a consumer. This is a conversation, and workflow can always be modified later. The good news is when you implement our solution, it is one implementation, and so our customers have the ability to tune what friction they put in front of their consumers at a later time as they learn what works.

CEOCFO: ***So, it is one solution you offer and then an organization can choose what areas they need?***
Mr. Geiman: Yes. Our customers can decide on which components to use but all of those components only require one integration.

CEOCFO: ***What is the business model for Confirm?***
Mr. Geiman: Today, our business model is transaction processing based—customers pay per scan, with the price dependent upon which product is used. We have some partners that are starting to bundle our solution as part of a SaaS offering and we are starting to price some of our services on a SaaS basis as well. But, for the most part, our business model is a transaction processing model based on what level of authentication a customer does and how many scans a customer performs.

"Thirdly, our customers have, in many ways, had no choice but to look for other mechanisms like Confirm to authenticate identity that are different than the traditional methods because the growing threat of cyber security data breaches have put a lot of pressure on customers to change their business processes."- Bob Geiman

CEOCFO: ***Who would be reselling your solution?***
Mr. Geiman: We have two primary categories of resellers / partners. Take Experian and Neustar; they are both large players that sell a number of different identity fraud and analytics services to financial services, insurance companies, retailers, healthcare providers, etc. These companies are adding our solution as part of a multifactor identity fraud strategy and offering. Our partners like what Confirm is doing because we are at the tip of the spear--the first thing that happens in the consumer lifecycle is the remote identity proofing process at the front end of opening a bank account or applying for a credit card as an example. Enterprises need to know consumers are who they say they are. If a partner can win the remote identity proofing business, these partners are better positioned to sell additional services downstream that are a part of their current product offering. That is one kind of channel—existing, large players in the identity and fraud space. We are also closing channel partners from vertically focused software players that provide an end to end workflow. iPipeline is a great example. iPipeline is a vertically focused SaaS company that manages an end to end workflow for the life insurance space. Large life insurance companies like MassMutual use iPipeline to manage the underwriting process: the relationship between the broker and the consumer, the relationship between the underwriter and the consumer, and the relationship between the broker and the underwriter. iPipeline has added our authentication capabilities as a part of a broader suite that is highly focused on that particular vertical. We have another OEM partner that is in the healthcare space…same idea…this partner sells a set of software services that support a number of different IT processes, soup-to-nuts, for hospitals. This partner uses our technology as part of the registration and intake process, pharmaceutical compliance and eventually billing.

CEOCFO: ***Would you explain how people are getting the information to make commit identity fraud?***
Mr. Geiman: 75% plus of existing identity authentication and fraud prevention business processes use challenge questions (what is your social security number, DOB, address, etc.) or passwords/PINs as the primary means of authentication. These kinds of solutions largely drive how businesses interact with consumers who need to assert their identity. The problem with those solutions is some enterprise needs to store the data, so enterprises can match your answer to the database. The basis of most cyber security breaches is capturing this data. If a bad actor, whether it be a state actor or a criminal organization, captures this data, that actor can either sell that data or use that data to commit fraud, such as account takeover. As an example, a bad actor uses this stolen data to get into your bank account and wire the money somewhere else. Consumers should presume that all of that data has been compromised. There have been enough large-scale data breaches that it is now safe to assume nearly every consumer has been impacted. That data has all been compromised and of course that data is the primary mechanism by which companies keep your account safe. It is a concern.

CEOCFO: ***Do you envision a point where consumers might look to do business with companies that protect their identity more than others?***
Mr. Geiman: I think we are getting there. Based on the last high profile data breach, the number of consumers that have frozen their credit is at a record level. Large enterprises are starting to market their corporate brands on the basis of trust in the digital sphere. We have seen a number of large RFPs from banks that are looking to replace traditional methods and move to next generation, artificial intelligence-based decisioning engines to avoid having to store raw data about consumers that enterprises do not need. The other thing that is happening is executives are losing their jobs, whether it is fair or not, over cyber security breaches. There is a great deal of congressional attention on the fact that all this consumer data has been breached and so much of the world's business processes are predicated on using this data. I think there is a lot of attention on these issues. I cringe when someone asks me for my social security number for the purposes of authentication; I know that number has been compromised.

CEOCFO: ***What is next at Confirm?***
Mr. Geiman: We are still only a little over two years old and a lot of our focus is on converting our pipeline to paying customers. We have also closed a number of large partners who are selling our solution and we need to help make these partners successful. We are in trials right now with a number of companies of significant size and substance. We have a very robust pipeline in early stages of development. We will not convert all of these but we will close our fair share. The second focus is where we take the product from here. We are doing a lot of work around how we extend the initial identity proofing process at the front end of a consumer relationship and integrate that process with downstream fraud management and consumer enablement. We have products that will help our customers confirm that a transaction that a consumer wants to initiate is a legitimate transaction. Becoming a larger part of the downstream re-authentication expands the total market opportunity for Confirm.io. That is our focus—customers and product. There are some other artificial intelligence initiatives that we are funding that will extend the use of some of our existing decisioning engines that we have built. It is still early days, but it is around extending our approach and capturing a bigger piece of identity and fraud management space.