Podcast with Gary Shiffman, CEO and Founder of Giant Oak

*Note that transcripts may sometimes contain errors and that transcript timing notations do not match the posted podcast

Jo Ann Barefoot:	00:03	I'm very excited to say that my guest today is Gary Shiffman, founder and CEO of Giant Oak. Gary, welcome to the program.
Gary Shiffman:	00:12	Thanks Jo Ann, great to be with you.
Jo Ann Barefoot:	00:14	I'm excited that we're finally setting this up. We both are actually based in the Washington area, but we ended up doing this by phone today because things are so busy. But we've been crossing paths for quite a while now as we've looked at the technology issues that are changing banking. I'm really excited to be able to have you on the show to talk about AI and to talk about anti-money laundering and to talk about anything else you want to talk about.
Gary Shiffman:	00:44	Great, and yeah, I've become a big fan and follower of yours since we've met at the last couple of years of conferences and I'm very excited to be on the podcast with you.
Jo Ann Barefoot:	00:44	Great.
Gary Shiffman:	00:53	Thank you for the invitation.
Jo Ann Barefoot:	00:53	Yeah, fantastic. Let's start talking about you. Tell us your background, how you got in to this field. I know a little of your bio, it's a very interesting one, and then tell us about Giant Oak.
Gary Shiffman:	01:08	Great, thank you. Yeah, so I come out of the National Security world and academia so I started my career in the US military. My first job out of college was the Gulf War, and then I went on and got a PhD in economics. To me, economics is about modeling human behavior, mathematical representations of human behavior. My life's work really revolves around the application of behavioral science to illicit activities. By illicit activities I mean fraud and corruption and money laundering and terrorism and trafficking, drug trafficking, human trafficking. The common denominator throughout my career is this interest in illicit activities and the application of behavioral science to the domain of illicit activities. And then about nine years ago, I started working on some projects at DARPA, and

DARPA is the Defense Advanced Research Project Agency, it's where the U.S. Defense Department spends a lot of money every year on research and development. So I've had about nine years of experience supporting DARPA research and learned about and developed expertise in machine learning and artificial intelligence.

Today, Giant Oak is really the culmination of knowledge of illicit activities, behavioral science, and the application of technology, specifically, artificial intelligence and machine learning, and building software so that people can benefit from the knowledge of the conjunction of those three fields, without having to go out and pursue PhDs or advanced degrees in these things. It's about democratization of this knowledge through the building of software. I'm thrilled, I think I'm the luckiest person in the world that gets to work on something so meaningful every day and it's a blast. I'd add that I'm also a professor at Georgetown University here in Washington, D.C. and so when I'm not at Giant Oak with the software team and the scientists, I'm over at Georgetown participating with the next generation of leaders and love every minute of that as well. That's me in a nutshell, I guess.

Jo Ann Barefoot: 04:03 That's great. Did you say what department you're in at Georgetown? Maybe you did and-

Gary Shiffman: 04:03 Georgetown, I teach in the School of Foreign Service, and I teach undergrad classes in International Economics Department and graduate classes in the Security Studies program. I teach classes on the Economics of Organized Violence, that's the core of what I teach, and I also teach a course on Econometrics and Causal Inference for National Security Professionals. Those are the two courses I'm teaching this semester.

Jo Ann Barefoot: 04:37 Actually, let's take another moment on that. The Economics of Organized Violence, tell us more about that?

Gary Shiffman: 04:47 Yeah, thanks. In fact, if it's all right I will plug that I have a book coming out with this title later in 2019 from Cambridge University Press.

Jo Ann Barefoot: 04:58 Great, we will link to that in the show notes and encourage everyone to buy that, and I'll buy it.

Gary Shiffman: 05:03

Awesome, thank you. We tend to think that the rules of economics apply to people in the elicit world, but not people in the illicit world. So I have spent years working on developing the base of knowledge to counter that idea. The example is, Jo Ann, if you and I decide to open a restaurant together, we need to generate revenues, revenues need to exceed costs, we need to hire, we need to recruit, we need to retain, and we have to do all of the things that go into running a business, make payroll. Even with all of that, there's a 50% chance that we will be out of business in three years, just because it's just risky starting small businesses and restaurants. If instead of opening a restaurant we decided we wanted to take over the heroin market in the portion of Washington D.C., all of those same rules apply. We'd have to do recruiting, retaining, we'd have to make payroll, we'd have to generate revenue and make sure revenue exceeds costs.

There's an equally likely, if not a greater likelihood, that we would fail and so my work in this field of the economics of organized violence is that if organized groups or groups that engaged in the sustained provision of violence have to abide by the same laws of economics. If we want to counter these groups, if we want terrorist groups and insurgent groups and drug trafficking groups and other transnational criminal organizations to fail, then if we treat them as a business, we know how to cause or at least encourage their failure. I think those of us in law enforcement national security, would do much better to think about the economics of these organizations and not simply think of the kinetic methods for countering the groups and the leaders. Does that make sense?

Jo Ann Barefoot: 07:22

Yeah, that is so interesting. I want to go back to tying this into the work that you're doing. First, just give us a little bit more about Giant Oak, whereas describe the business, where you are in your growth cycle?

Gary Shiffman: 07:38

Yeah, great. As I said, we were doing research, government funded research with DARPA going back to 2009 to 2012. Then it was in 2012 that we realized that instead of just doing the research, we could actually build software and have a bigger impact in the world, and knew people could use our software. we became a software company in September of 2012 and it took two years or until September of 2014, for us to make our first software sale. We sell a SAS product, software as a service,

and it's called GOST, G-O-S-T. It's been available and sold enterprise grade, enterprise level software since September of 2014. That was our first customer, our first sale. Since then it's been growing regularly organic growth month over month, and it grew through word of mouth, usage of GOST. As we got more customers, we would invest more in the product and get more customers invest more in the product, and we really didn't spend any time on sales and marketing.

We have zero churn meaning nobody quits the technology once they start using it, it's very powerful and user friendly. But six months ago or late in 2018, we decided that it was time to actually invest in sales, marketing, and a little bit more on product development. So we took a Series A round from Edison Partners out of Princeton, New Jersey, and so we now have been growing through the hard work of sales and marketing. Edison Partners it's a venture capital fund in Princeton where two thirds to three quarters of their portfolio is in FinTech and RegTech. This is a very important part of our future and so we decided to work with Edison for the purposes of not only getting the capital to support growth and taking a growth equity round, but also taking the growth equity rounds from folks that knew the FinTech, RegTech space extremely well, understood how to work with innovative growth stage technology companies. We're about five months now into that relationship with Edison and loving it and seeing the benefit of their expertise as well as the capital and that's where we are today.

Jo Ann Barefoot: 10:39 Fantastic, how large is your team?

Gary Shiffman: 10:43 We have over 30 employees right now. Just to give you some context, January of 2018, so just over a year ago, we had about 13 employees so we've more than doubled in the last 12 months and the pace of growth is continuing. We're very excited about all of this, and of course, we're very busy as a result of this. You work very hard to try to double the size of your company and then you realize how much work goes into the company now that it's doubled in size. We're dealing with all of that, we have new offices and really enjoying that. But you have to do things like staff or buy snacks for the kitchen and buy desks and computers for people, and so we're going to all of those types of growing pains, which to be honest, is just a lot of fun.

Jo Ann Barefoot: 11:46 Good. What exactly does GOST do?

Gary Shiffman: 11:54

GOST stands for Giant Oak Search Technology, G-O-S-T is how it is spelled, and GOST is used for large scale screening, vetting, and continuous monitoring. Screening, vetting, and continuous monitoring happens in a lot of places in a government agency or in a bank, so it can be for onboarding new customers, it can be used for risk refresh for existing customers. Any sort of applications or any sort of a benefit, GOST can be used. It's uniquely capable and was built to solve the problem of scale. The concept here is that the world is awash in data today, and that's a wonderful thing except that, that is too much data and we're overwhelmed by it. When it comes to looking for signal and noise or looking for indications of threats or risk for the absence of threat, we tend to go to highly curated locations for that data. We look at the data inside of the bank, for example, and if we look at data outside of the bank, we tend to go to list providers.

The state of the market as I saw it was one of name matching across curated lists. That's nice but you're still only looking at a very, very small fraction of the data in the world and data that could ultimately prove very valuable for your enterprise in terms of identifying risk, identifying the absence of risk, or finding money laundering, drug trafficking, fraud, corruption, insider threats, things like that. GOST really exploits what's called publicly available information. You can think of it as the internet or the World Wide Web, we call it PAI or publicly available information. If you want to think about how you're using PAI inside of a financial institution today, you're primarily using it for an investigation. Meaning I've already narrowed down a massive population to a small percentage and now I'm going to do investigation, I'm going to do customer due diligence or enhanced due diligence and then you're going to go to PAI.

GOST allows you to use PAI or publicly available information at the screening mode and not wait until you get to the investigation phase. If you're onboarding 10,000 clients a day, or 1000 clients a day or 100 clients a day, it doesn't matter because you don't have the staff on payroll to run a Google search or a Bing search on all of those people. If you're a large bank and you're onboarding 10,000 a day, you can't hire enough people to run the 10,000 Google searches a day to deal with the false positives, capture data, push print screen, cut and paste, create some sort of a dossier, very time consuming process so

you end up not doing it at the screening phase. GOST does everything that I just described, so you run the 10,000 entities through GOST, you run the entire population of 10,000 through GOST. GOST, because it is so good at PAI, it actually benefits from a process in which we reindex the internet and you gather the data on the entities that you're screening. GOST then machine reads everything and does a prioritization.

You get your query in as 10,000 entities, the output from GOST is a rank ordering from 10,000 down to germaneness irrelevance. If you're interested in money laundering, it's going to rank order information that is deemed germane to money laundering or anti-money laundering. Now you have your team and they can go through the publicly available information as retrieved by GOST, and they don't have to look at all 10,000. As an institution, you don't have to look at zero, you can determine you're going to look at the top 1% or the top 100 or whatever rule that you as the bank sets up. Now you've got a repeatable, defensible, disciplined process for looking across internet space for information germane to your mission such as money laundering.

Jo Ann Barefoot: 17:24 Great. That's an interesting term, reindexing the internet.

Gary Shiffman: 17:30 Yeah.

Jo Ann Barefoot: 17:31 That's the first to the sequencing by risk I gather.

Gary Shiffman: 17:37 If you think about, if I can explain it for a second, because you're right, that's a big word and I just threw it out there without support. Let me go back and fill in a little detail. When you think of the internet, Jo Ann, you're actually not thinking of the internet, you're thinking of the domain meticulously curated by somebody like Google or Microsoft. The internet is not something you access directly but you access it via one of the search providers. They index, the estimates are, is that they index less than 10% of the internet. Nobody really knows because nobody knows how large the internet is but if we go with a number like 5%, so Google has or being or somebody, one of these general purpose search tools. They've got 5% of their index. That means when you think of the internet, you're only imagining 5% and not the other 95%, and the 5% that's indexed is indexed to optimize the business model of the search provider. If you're working in a Google, they're an online ad company.

So they've index the 5% of the internet that's likely to optimize eyeballs on web pages, so they can sell ads. It's a phenomenal tool, it's a great tool, I use it every day, and I'm sure you do as well. However, if you're looking for money launderers, it's suboptimal, it's not optimized for A amount, it's optimized for shopping. What GOST does is it reindexes the internet but not for shopping but for AML or for other used cases that our customers have. When I say reindexing the internet, I'm talking about bypassing the general purpose search tools and going to a bespoke custom internet. You, Jo Ann, get your own custom internet, not the one that somebody else built for 100 million unique users today but built for you and your enterprise in what your unique search and retrieval requirements are. That's what GOST does, and because GOST can do that ... and that's very unique, that's not a lot of people can say they can do that. Because GOST can do that, then you can build analytics on top of it that allow you to do screening, vetting for onboarding and customer refresh.

Jo Ann Barefoot: 20:20 So interesting. I want to talk in a couple minutes about where we're going overall with both AML policy and regulation drawing upon AI. But before we do that, how do you assess the readiness of the compliance and regulatory community to try tools like this? They're so new at least compared to the traditional ones, and you're trying to ... as you just pointed out, you're doing something that's quite unique, what is that barrier like if you encounter it and what are the ways to develop the trust and tools like this that people frankly don't really understand how they work?

Gary Shiffman: 21:12 Yeah, great. Thanks for asking you that, that's one of my favorite things to talk about, which is, believe it or not, it's really the technology is awesome and I'm so passionate about the technology but I really want us to change the world. To change the world we need to, A, have the technology but we need to address what are the burdens to actually making the changes and having technology adopted and deployed? I really believe that there is no villain in this story, I have yet to meet somebody who says, "No, I absolutely oppose innovation and change in the regulatory compliance world." Nobody has ever said that and I haven't found anybody who I believe feels that way and just avoided to say it. I have spent hours with bank regulators, with Treasury Department officials, with health staffers, and I know you have as well, Jo Ann and I don't know if you've had the

same reaction I have. But everybody I meet with, and I'm just talking generally about the evolution of technology and data and artificial intelligence and machine learning.

People are excited about this, so I'm really having a hard time finding the pushback. I think that the joint statement by the OCC and FinCEN and the Federal Reserve and other regulators that came out in December was a fantastic indication of this. If you remember, and I know you do, that these agencies, in fact, they did it at the ABA Financial Crimes Conference when we were there in December at the Gaylord Resort in Washington, D.C. They basically said that they encourage or they support banks experimenting with these technologies, artificial intelligence and machine learning. I think everybody understands that these technologies are transforming every aspect of our lives. They are, I mean, that smartphone that you carry around with you is enabled by machine learning, it is enabled by artificial intelligence, and it's impacting every aspect of your life. To think that it's not going to impact AML/KYC is ridiculous.

I think the untenable position is to think that AML/KYC is not going to change because of technology, because every aspect of our life is changing, it will absolutely impact AML/KYC, completely convinced of that. Yes.

Jo Ann Barefoot: 24:17

Let me just pause you there, I'm making a speech tomorrow night actually on AI and regulation, and that's exactly what my talk says. The crazy thing is to think that we're not going to have these technologies come into regulation alone. Everything else is going to be changing but somehow regulation is going to sit there using its ancient model. That is impossible, getting from here to there may not be easy in some cases. The other thing I want to say is I agree with you on that wonderful interagency statement that came out in December and we will link to that in the show notes. It was extremely significant both because it proactively encourages use of RegTech for AML and including pilots and experimentation.

Secondly, because it did come out from FinCEN jointly with the FED, the OCC, the FDIC and the NCUA, which is really a very, very powerful step forward in terms of getting everyone to know that they have permission to try new things. The industry is for good reason, they're cautious with their regulators and it was just so constructive to put that statement out.

Gary Shiffman: 25:41

Yeah, I couldn't agree with you more and I love being in your choir here, and as you're out preaching the word on change. I love what you do, I appreciate what you do and the speeches you give in the podcast and everything. Because, like I said, we're in this to change the world and the technology is there, people are excited about it, we just need to work through. We just need to work through the inertia to answer the question. This is an environment of low risk, so banks and bank regulators tend to be low risk cultures, and so change comes slowly. That's not a bad thing, I think we just need to be aware that change is going to come slowly. Then we need to go into this with the understanding that this will change, absolutely will change, and we just got to work at it. The key to that, Jo Ann, is data, its empirical proof is my approach to this. I could give a 45 minute lecture on why AI and ML are going to make, AML, anti-money laundering, know your customer, orders of magnitude more efficient.

But it's just that, it's just a theory, it's just the electrodes, it's just an argument. What I believe we need to do is we need to do hackathons, we need to do experiments, we need to run tests. And then based upon those, we need to generate data and then the data then needs to be presented to the regulators, or better yet, and I know you did that awesome podcast of your experience in the UK. But we need to bring the regulators and the oversight folks into the room during the experiment, let them see the results after the experiment, and that will be blatantly clear to everybody involved that the application of these new technologies to the RegTech space actually deliver on the theory, they do work. That will move, that will move us forward and generate force acting on that inertia to get us to move forward.

Jo Ann Barefoot: 28:21

Yeah, I couldn't agree more. There's going to be another great hackathon, pardon me, as you know, they call them tech sprints, coming up in London this year. Even bigger and better than the last couple, which is really saying something. This is so exciting to me. Let's widen the lens and just talk a little bit about your vision for how AI and machine learning will be used to solve problems above and beyond what you're currently doing in the AML space. Maybe more broadly on regulation in general, what's, I'll put you on the spot a little bit, what's the vision? What's the opportunity look like?

Gary Shiffman: 29:13 Yeah, so for me, yeah, you're totally putting me on the spot, but I'll answer it, I'll answer it anyways. Machine learning is moving us into a world where the algorithm is trained by the data. Humans have heuristics, and based upon those heuristics, we build the models and that's wonderful and I never want to move beyond that. However, we're much better at the building and the development and the evolution of our models to the extent that those models get trained by more and better data. The upper bound of model performance is it becomes a function of the quality of the data used to train the model, right? Are you with me so far?

Jo Ann Barefoot: 30:08 Yes.

Gary Shiffman: 30:12 What we need to be thinking about is how we generate the best data for training AML models, if we're going to optimize anti-money laundering. The current regime we have in place under the Bank Secrecy Act for AML and as well as for KYC and sanctions and fraud and all these things, that the current regime we have in place hold things individually responsible and accountable for the development and building of their programs. Make sense, except for the fact that the technology within the bank can only be as good as the data within the bank. If you are a small bank, a regional bank, a bank with a focus to your customer base, then you're going to have a focus to your data, and so your model building will be limited by the data that you have available to train your model. You can't share that data or you can't share it easily but you probably can't share it at all with other banks for the purposes of sharing knowledge, sharing best practices, but really for building better models. I think where we need to go with this is we need to find clever and creative ways to bring data and algorithm together.

I need an algorithm and I need the data and I need the algorithm and the data be at the same place at the same time so I can train the algorithm. There are several ways to do this, I'm working on one of the ways towards creating a utility, which is a shared ability to collaborate across things in order to build the best models that is only now available to us because of the evolution of machine learning. That's where I think we need to go, I think we need to think about leveraging technology to build better models taking advantage of data. Data is the key to all of this, it's really all about the data these days.

Jo Ann Barefoot: 32:34

This is fascinating. One of the things that the FCA, again, we're talking about the UK Financial Conduct Authority has taken a lot of leadership in this field, and we'll link to those shows in the show notes as well. As you know, one of the things that they have been emphasizing and so have others is the question of how are we going to solve the privacy problems? If you just widen the question a little bit, we know that in AML, specifically, the criminals are winning that battle, the UN says we're catching less than 1% of the crime. We know that a primary or the primary reason for that is that the industry and the law enforcement entities can't look at all the information and find the patterns. We know that machine learning could find them if they had enough, if the computers had enough data.

The hang up is that the good guys can't share data freely because we have to protect people's privacy, we can't just willingly put out information across the whole system that would say that somebody was suspected of a crime or all the other ways that privacy could be compromised. I know the FCA is working on this, how do we solve the privacy issue and then enable the much greater connectivity of data that you're talking about?

Gary Shiffman: 34:21

Yeah, so my solution to that is something called the traveling algorithm I've been, as you know, I've been working on this for over a year now and working with the Bank Policy Institute here in the United States, used to be the clearing house, now the Bank Policy Institute. The key ideas we have to get algorithm data in the same place at the same time, everybody's been focusing on moving data, but as you say, there are a lot of restrictions on moving data, privacy, civil liberties. Plus as a technologist, data is just big and clunky and sticky and it doesn't like to move, it's hard to move a terabyte of data or a petabyte of data, it's very difficult. My solution, my approach to this is everybody's data stays at rest inside of their own bank and we share an algorithm and we share algorithms and those move around. As they move around, they get smart. When the algorithm ... If you're that regional bank with a regional focus and not a lot of diversity in your customer base, then you don't have a lot of diversity in your data.

But you can build a great algorithm for the customer base that you have, but if you can share that algorithm with other banks, those other banks will benefit from your customer base and

you'll benefit from the models built on their customer base. So now you have collaboration across banks without sharing personally identifiable information. That's one way to address the issue of the regulators, the regulatory burden on sharing of information. There are other initiatives underway, one is create data lakes where all of the banks share all of their data. There you have to address the privacy concerns, and the third is in the U.S. context anyways, it's 314(b) under the Patriot Act, which provides a safe harbor for banks to share data. PII data across banks but really 314(b) applies in that, and when you're in investigation mode, you already have the lead, you're already working a case. Using 314(b) allows you to share the PII because you already have a predicate.

We're not going to increase much above that 1% of, less than 1% of crime that we currently find that you quoted on 314(b) alone. 314(b) is wonderful and I encourage expanded use of it. But really it's about large scale collaboration and I believe and I'm building out the traveling algorithm method for doing that.

Jo Ann Barefoot: 37:24 I knew you were doing some of this but I didn't know all of it, I'm really excited to hear it. This is such an important point, even though you just said, I'm going to reinforce it.

Gary Shiffman: 37:33 Yeah.

Jo Ann Barefoot: 37:34 That state the leading thinking in this space is that instead of bringing the data to the analytical tool, we take the data to the ... and we bring the algorithm to the data, leave it where it is. That solves so many problems of risk and concern, if you're not centralizing and creating these huge honey pots of data that are vulnerable to hacking and everything else. This is doable now, this again this is very central I think to the work that the FCA is doing, or at least the concepts that they're working on. I hadn't heard a call to traveling algorithm though before, I love that. When you said earlier that you're working on creating a utility, I think when people hear the word utility, they're usually picturing a big government run or quasi government blessed database. But that's really not what you're talking about.

Gary Shiffman: 38:35 No, not at all. The utility is I'm envisioning it will be owned, run, managed by banks themselves, so it will be maybe a collaborative which banks will voluntarily choose to participate in or not. Through participation, you get access to the traveling algorithm and you get the benefits of the traveling algorithm.

Any return on investment you would get from machine learning in your own bank will be increased by participating with the traveling algorithm because, again, the models will be better because it will be trained across more data.

Jo Ann Barefoot: 39:19 Exactly.

Gary Shiffman: 39:20 So very simple concept.

Jo Ann Barefoot: 39:24 Okay, this is fantastic. The other point I want to reinforce that you just said is that most of the models today have been focusing on trying to find people who may be engaged in money laundering and then searching their connections and all that. But this emerging emphasis is saying if we can anonymize the data, we can get it encrypted or protected and let the machines find the patterns in it without needing to show that PII to human beings who are analyzing it unless and until patterns are turning up that warrant a closer look. And then law enforcement, which doesn't have enough resources and the banks as well, can go through whatever is the appropriate due process to look at PII on some of these more robust sharing models. Go from there, but they'll be able to use their time efficiently.

Gary Shiffman: 40:29 Right, right, no, that's exactly right. That's exactly right. If you go back to where we started you asked me about my background. I'm a behavioral scientist, I'm interested in patterns of human behavior and that's so, so critically important to the future of where we're going here is understanding how patterns of human behavior are indicative of the types of signals that we're looking for. It's not the name that matters, it's the way in which people behave that matters. And adding behavioral components to the normal biographic ways in which we approach these problems is another aspect of the future in where we're going.

Jo Ann Barefoot: 41:17 Yeah, and you're the expert on this but my understanding is that a lot of the science is coming from the capabilities that companies like Google and Amazon have developed for understanding patterns of consumer behavior in order to target ads to us or whatever. That type of behavior modeling can be applied to find the behavioral patterns of financial crime including some types of financial crime. Human Trafficking doesn't look like weapons trafficking doesn't look like

endangered species trafficking. You can see in the data what is probably going on if you have enough of it.

Gary Shiffman: 42:01 Right, I agree. I wouldn't say that the idea's coming from them, I would say that they're proving out the model, right? Amazon recently announced a trillion dollar valuation. They're not worth that much money because they deliver books overnight, they're worth that much money because they have these exquisite models of human behavior on each and every one of us that our customers on their platform. That allows them to generate massive amounts of revenue. But I don't do that for a living and I don't care to do that for a living but they've proven the model that taking all of my data to build the models of human behavior actually provides a really large return on investment that's scalable, and they've proven that point for us.

Jo Ann Barefoot: 42:52 Yeah, well said, great. I know we're going to run short on time. Let me just ask you, I'm so enjoying this conversation. Open ended, what else should we talk about? Again, our audience is keen to understand AI, in particular, and how we're going to move into this new world, what are the opportunities? What are the risk? What else would you like to say?

Gary Shiffman: 43:23 Yes, so I think in order for us to realize this ivision that we're talking about, Jo Ann, I think there is a role for the government to step up and help out and that is on doing a better job of sharing what I call ground truth data back into the banking world. If you go back to this idea that your machine learning model is going to be as good as the data that you use to train it, a bank this year is going to send 1,000 or 10,000, or 100,000 SARS to FinCEN. They don't know if any of those sars were good or bad, they don't know if any of those sars led to high level trafficking organization arrests or low level crime or nothing at all. To the extent that we can get feedback from the agencies back to the model builders and the banks or in the utilities, it's going to be much more efficient.

I think that's one of the things that we need to work on, which is there's a triangle, you've got the legislative intent behind the Bank Secrecy Act is to generate data, is to require or empower banks to generate data for law enforcement and national security purposes. Regulators are there to enforce the law and regulation, but it's not being done for the purpose of the regulators. We don't do regulatory compliance for the sake of regulatory compliance, we do regulatory compliance to

generate data to help the law enforcement and the National Security communities. There's three players, there's the bank, there's the regulator, and then there's law enforcement. We need to close the loop, we need for law enforcement, after they get the data via the regulatory process, they then feed to provide feedback back to the bank and say, "Hey, I want more of this, less of this. Then the bank can tweak the models, then the regulator can make sure that, that process is happening.

And then law enforcement gets a new round of data and hopefully they're happier with the data that they get, they get more data, they get better data, they get the data that's more on point and less off point. I think we really need to work on closing this communication gap so that law enforcement, A, provides feedback on the data, on the cases. SARS are the way in which we report the data today, but there's no requirement that there will always be SARS, but this data has to come back. Get the law enforcement and the feedback has to get back to the bank, and the other thing that I think that ... and I come from the law enforcement national security world, so I'm not throwing stones, I'm talking about my own background, but we need to also give priorities. We need to give feedback and say, "Hey, this was good, this was bad, give me more this." I think it'd be great if law enforcement also said, "For next year these are my priorities." If the regulators could then give banks credit for responding to those priorities.

Because if you take a step back, Jo Ann, and you think about why are we doing all of this? Why do we have an AML regime in the first place? Why do we do KYC in the first place? It's for public safety, it's for security, it's to make us all safer. I think we lose sight of the big picture goal here because we get so caught up in our SAR filing rates and things like this. Let's take a step back and think about we want to build better models so that way we can generate better data for people who do security and make us all safer. If we did that, we'd understand that machine learning and artificial intelligence actually require feedback from the ultimate consumers of the data to say, "I want more of this and less of this."

Jo Ann Barefoot: 47:43 Yeah, this is so important. There's a tendency for people to think of money laundering as white collar victimless crime, procedural crime, but it is funding some of the most terrible things in the world: human trafficking, terrorism, again, animal and weapons and drug trafficking. And incredibly lucrative

businesses and they would not be lucrative if they were a high risk of being caught at them. Back to your economics points that you started with earlier. We can do better than we're doing, everybody, the technology's there, I think people realize that. It's important. But to bank the feedback loop work, I think one of the practical issues that comes up is if the law enforcement agency says to the bank, "This SAR was very helpful." In a situation where they're not asking for more for follow up information, they just are giving it a gold star, people worry that, that would be hinting back to the bank of that they're interested in the people involved and that starts to throw you into the privacy problem. Is there a solution for that?

Gary Shiffman: 49:14 Yeah, I think just good communication can help mediate that issue, which is this pattern of behavior was super helpful, this case, this SAR was helpful, this information was helpful because of the pattern. Because of not the name specific because we're not building in this machine learning world, I'm not building models based upon names and building models on the pattern of behavior. If law enforcement can say, "This is the pattern or behavior I'm looking for," and this ended up being very productive in terms of generating a lead for a new case leading to a prosecution in existing case, I think we can do that in that context. One of the things you might do to facilitate that conversation is designate somebody within the bank that has access to sensitive information. Clear them for law enforcement sensitive discussions and then you can have that give and take and back and forth.

Jo Ann Barefoot: 50:28 That's a really interesting thought, I've never heard anyone say that before. This is so great. Again, we're just about out of time, anything that I haven't asked you that you want to talk about? Any advice for anybody? It's always a good ...

Gary Shiffman: 50:47 Yeah, so my parting comment will be in saying this with you is just so perfect. But don't think that we're not going to be able to make big changes and change the world here because I think we absolutely will, and there's so much enthusiasm right now for the impact of technology in regulatory compliance, in generating data for public safety and public security. I think 2019 is going to be a very big year for this and anybody listening that's remotely interested in this topic, don't doubt it, just believe that we're going to be contributing to some big changes and this is an exciting time in history, this is a big movement.

Don't be discouraged or deterred because this will happen, this will absolutely happen, we will be successful.

That's to all of your listeners and to you, Jo Ann, thanks for the amazing leadership role that you've played in bringing us all along this far. This is an exciting time. I'm thrilled to be a part of it, I'm thrilled to be in your network and be on the same team as you and I look forward to seeing a lot of big changes in 2019.

Jo Ann Barefoot: 52:19 Well, thank you. You are inspiring me and I've also learned a lot in talking with you today, which is just fantastic. Where can people get information about Giant Oak?

Gary Shiffman: 52:29 Our website is giantoak.com and that's the best place to go. You can also find me on LinkedIn if you want to reach out to me directly, if you want to get to me, but giantoak.com is where you can find all kinds of information on me, my team, and our company.

Jo Ann Barefoot: 52:47 That is fantastic. Gary Shiffman, thank you for being my guest today, it's been fantastic.

Gary Shiffman: 52:54 Thank you, Jo Ann.