Unauthorized Access*: *Snooping Sadia Talks to Former Official Gene Fishel
Host: Sadia Mirza
Guest: Gene Fishel

Sadia Mirza:

Today, I'm joined by Gene Fishel. He's a frequent NetD speaker, former regulator, and now a member of Troutman's Regulatory Investigations, Strategy + Enforcement Practice, also known as RISE. Gene, thanks so much for joining me today.

Gene Fishel:

Well, thank you, Sadia. It's a pleasure to be on and thank you for having me. I'm a longtime listener and honored to be featured on *Unauthorized Access*.

Sadia Mirza:

Gene, I love it when people say that. I think we're about eight or nine episodes in – so, that's perfect.

Gene Fishel:

Well, it's been a great eight, nine episodes.

Sadia Mirza:

Exactly. Gene, I need to tell you something. Last week, I was in the Richmond office, which is where Gene sits, and I spent a lot of time admiring all of the trinkets in your office. Yea, I did. I read everything. I looked at, I think if you had notes on your desks, I probably read them. But you have – one, I love the Richmond office because everyone's office looks like they've lived there for the last 50 years at this point. And it's so well decorated, and every – it's so different to Orange County, which is in California. Because our office, they're very clean. And not to say that your office isn't clean, but there's nothing – nobody really decorates their office like the attorneys in the Richmond office where everyone added their own – you could tell everyone's personality.

Gene Fishel:

Right. Well, we have to make up for things with our office, because we don't have the weather you all have in Orange County.

Sadia Mirza:

That's true.

Gene Fishel:

And we spend a lot of time in our offices, whereas I'm sure you all are outside having a great time.

Sadia Mirza:

Well, you know what, I do think that there's a difference, and I bet more people work from home in the Orange County office, because I think Richmond was a little bit busier. Anyway, I walked out of your office thinking that you are the most interesting man in the world.

Gene Fishel:

Well, I'm not. But thank you for that.

Sadia Mirza:

Oh, for sure. And there's even, if I wanted to decorate my office, I just decided I wouldn't, because I don't have as many ornaments to put up in my office.

Gene Fishel:

I will say this, when you work for the government for 20 years, you collect a lot of trinkets, and plaques, and coins and that sort of thing. It kind of makes up for other deficiencies.

Sadia Mirza:

Okay. Yes, so your coins, that's what I wanted to ask you about. One thing I want you to do is tell the listeners a little bit about your background, because I think it is very unique, and it's very helpful, and we're going to talk later on, about our incident response practice. But I specifically want to know about the coins and what I need to do to get them.

Gene Fishel:

Well, so I spent 20 years in the Virginia Attorney General's Office. For 16 of those years, I was chief of the computer crime section. We had a dual role there. I managed attorneys and also a computer forensics unit, computer forensic examiners, and we handled both criminal and civil cases out of that section. We prosecuted, investigated and prosecuted cybercrimes across Virginia, in all jurisdictions of Virginia. And, on the civil side, we enforced Virginia's privacy statutes. So, database breach notification laws, and also parts of the Consumer Protection Act.

Parallel to that, I was fortunate to partner with the US Attorney's Office also for 20 years where I was a special assistant U.S. Attorney. So, I had the fortune of prosecuting hundreds of cyber cases in federal court, also in both districts of Virginia, which leads me to the coins because for those of you who have been involved in law enforcement know that anyone involved in law enforcement loves what are called challenge coins.

And so, and when you work, one of my goals, whenever I worked with a new law enforcement agency, I would ask for a coin if they didn't give me one at the outset, which a lot of times that

just happens. The first time you work with an agent, they'll a lot of times hand you their organization's coin. So, most law enforcement agencies, federal and state and local, will usually design some sort of coin that they hand out, that's kind of a token of appreciation. We had our own coins at the Attorney General's Office. Each attorney general that was elected would design his or her own coin.

It's a thing, where you exchange these coins, working with the different law enforcement agencies. And, I one day decided I need to get a nice little stand. They, of course, sell stands just for these challenge coins. And, I think last year at some point, I said, I need to display these things because it looks impressive, even though I'm –

Sadia Mirza:

Very impressive.

Gene Fishel:

That's the story of the coins. It's primarily a law enforcement thing. But I've been fortunate enough to work with, gosh, a variety of federal, state, and local agencies. I mean, dozens and dozens across the board in dealing with cyber issues.

Sadia Mirza:

Gene, I work with law enforcement all the time. Do you think they're going to be inclined to give me a coin if I start asking them?

Gene Fishel:

Yea, I think if you ask. And knowing you Sadia, I know they would be happy to give you, in particular, a coin. I think, it's more of a default action between law enforcement, that you hand these things out. But I have no doubt that the next time you work with the FBI or whatever, the FBI, they have a lot of money, so they have all sorts of coins. If you're working with the FBI, definitely ask those guys for a coin. They'll give you one. It's not just limited to a law enforcement.

Sadia Mirza:

Gene, did any law enforcement agent, say, declined giving you a coin?

Gene Fishel:

Declined me?

Sadia Mirza:

Yes.

Gene Fishel:

Not that I remember. Sometimes, you know how law enforcement budgets are. Sometimes they run out of coins. “Oh, we just gave out our last coin.” So, you may not get them for another year, because they've handed them all out. That kind of thing is tight as you can imagine in government. Sometimes, I definitely asked before and they've run out.

Sadia Mirza:

Okay. Wait, I hear you correctly. So, FBI, law enforcement, but the AG’s offices, they have their own coins, too?

Gene Fishel:

Yea, yea. In fact, next time, I think I have some spare ones, next time I see you, I will be sure to bring along some spare AG coins I have.

Sadia Mirza:

Gene, you should know, we have a great interoffice system at Troutman, and you can just send – we don't really have to wait that long.

Gene Fishel:

I actually have not utilized that since I've been here. For those listening, I've been here about seven months now. I joined the firm in June of last year, but I have not had a chance to utilize the interoffice mail system. Maybe I should put it to the test.

Sadia Mirza:

Yea, just test it out. See if it works. I will confirm on my end as soon as I get the coin.

Gene Fishel:

Okay.

Sadia Mirza:

So, let's add that to our list. Okay, one thing you said actually that was interesting to me was the forensic examiners that sit within the AG’s office. Are they forensic examiners like what I think in the traditional sense? You know if there's a cybersecurity incident, we bring in a forensic firm to do the forensic investigation. The AG’s office has their own forensic team essentially. They try to re-mimic investigations just to confirm scope? Or, can you expand on that, what is the purpose of that?

Gene Fishel:

They are what you probably think they are. They are computer forensic examiners that are in the AG’s office. They do mostly criminal work, criminal investigations. So, what they are doing,

the way it worked here in Virginia, an investigating law enforcement agency, say state police, Virginia State Police, or even some federal agencies would call them up when they are about to execute a search warrant, for example, at a suspect's house. Our forensics team, they actually had an RV that was a forensic lab, a mobile forensic lab. So, what would happen was the agents executing the warrant on the suspect's home, apartment, whatever, business, would bring out the seized evidence, and the forensic examiners would actually triage the evidence at the scene to determine what was of evidentiary value. And those items, if there's a laptop, or cell phone involved, that would potentially add value, the investigating agency would seize that item, and then turn it over to our forensic examiners who would conduct a full forensic examination on the device.

And so we had, not only do we have a mobile lab, in the AG's office, we had an actual forensic lab in our building that was specifically designed to conduct forensic examinations. So, they have all the, as you know, it's very capital intensive, they have all the servers, the software, the Faraday devices, all of that stuff to conduct full blown forensic examinations. They would conduct the examination, produce a report. And then, if it went to trial, they would testify as experts in the trial. They also did some civil work for estate agencies and that sort of thing. They would also go on scene, if called for, if there were large servers involved in businesses, which we see a lot in the data breaches. They will isolate segments and copy segments of the server and do a forensic examination off of the original server.

It's a little trickier, of course, when you're dealing with businesses with massive servers because you can't just pull up the server and take it back to the forensic lab. You got to image it at the business and then work off the copy. Of course, in forensic examinations, examiners always work off the copy. They never, or they shouldn't, shouldn't work off the original, because potentially, it could change the evidence or change what happens.

So, our forensic examiners did all of that. They were very good. Not every attorney general has a lab like that. It just varies by state. But fortunately, we had the funding to set something up like that to help law enforcement and businesses who were victimized by cybercrimes. It wasn't always a suspect, but sometimes our forensic examiners would assist victims in figuring out what happened, say on their server. With our clients, when they suffer a breach and you call in a firm, you're trying to figure out, really, what happened? You're trying to get to the truth. See where the access points were and what data was potentially compromised, that sort of thing.

Sadia Mirza:

Okay. This is so interesting to me, and I swear, you coming on board to Troutman was one of the best things to happen to me, because every time I'm dealing with an incident and dealing with the regulator, now I feel like I can pick your brain as to what are the regulators are really thinking. If I write something in a certain way, or present a certain set of facts, I have you in my pocket now to run things by. And I wanted to ask, when you used to receive reports of incidents, and I'm talking specifically like on behalf of businesses, what types of incidents, like initial reports you get, what type of incidents actually got your attention that you felt like you wanted to follow up on?

Gene Fishel:

Sure. So, in enforcing our privacy laws, when I was a regulator, we would get, and it would almost always revolve around a data incident, most likely a data breach actually. Organizations and businesses, as is the case in most states, not every state, but in Virginia, if an organization, of course, itself has suffered a data breach, they have to report it to the Attorney General's office in Virginia. So, we would get, as you can imagine, hundreds of such notifications a year where my attorneys and I would be responsible for sifting through these notifications to determine if an organization is complying with the notification statute. As you can also imagine, there are hundreds of these notifications where we look at them once, and that's it. Most companies, organizations now, especially today are hiring skilled counsels such as yourselves, and data breach incident response has now been perfected over the course of many years now, where the notifications have just steadily improved over time. I've seen that because I was there at the outset when our law was passed. But there are certain unavoidable facts, that will definitely raise our attention. The two most prominent that would catch my eye are the sensitivity of the information involved in the incident. So, something like social security numbers or health data, health diagnoses information, might garner more scrutiny than say, credit card numbers, for example. There are just two different kinds of data we're talking about, and the risk to consumers that are affected. It's greater, the risk of identity theft.

The other thing was the size and scope of the breach. That really just comes down to the number, the potential number of consumers affected. So, in Virginia, organizations have to notify if just one consumer was potentially affected. Again, it's different among states. Some states have a threshold where they have to notify the attorney general. But in Virginia, it just takes one. So, we would get notifications from one or a handful of potentially affected consumers to millions. Of course, the breaches that involves millions of Virginians, that is absolutely going to make me take at least a second look.

And I say this, having worked with attorney's general all around the country. I've worked with all of them. Regulators, when there's a national breach that is affecting most states, the breaches you hear about in the news, the attorney's general get together, and they have regular meetings where they discuss these incidents. And it's not always the case that a major breach is going to garner or kick off some sort of investigation. But the larger the breach is, the more likely that is to happen. But, again, that being said, it very well could be that a company, an organization, even if it's a large breach with sensitive information, has done everything right. They filed timely notice. They're sent out timely notice. They had proper security to begin with, which is something else, that now states are even more so starting to look at with the passage of these comprehensive data privacy acts. Or it could be that a company didn't take the correct steps. And, a lot of times, we determined – I keep saying we – but the regulators – I'm not a regulator anymore – but they would ask some initial inquiry, send out some inquiries with some general questions, trying to get some more information. And, if they're answered satisfactory, that might be it, the investigation is over. If not, if there's something peculiar about the processes, say, the organization employed prior to the breach or something like that, then it might lead to a full-blown investigation, and that investigation could involve every state and get 50 states and territories, 50 plus states. Or it could involve us a few states, maybe just – of course, a state's going to be interested if their citizens have been affected. But not every breach affects every state. A company that is headquartered in a particular state, that state might take an interest because of that. And so, there could be a variety of different makeups of investigating bodies, just depending on the incident. It could be dozens. It just all depends on the facts.

Sadia Mirza:

I told you that I didn't give you any questions beforehand, and it was going to be a very impromptu interview. I always know, we're already at the top of our time, but I'm going to, despite what everyone tells me, I'm going to keep pushing this forward, because there's two questions that I have for you. Maybe there's going to be a part two to this, because I think it's an important topic and something that I'm interested in, sitting from, given my practice. But, my first question is, is there something when, attorney's submitting the notification, or businesses submitting their notice to the AG, is there is something that a business could say, or an action that they could take as part of their response efforts that would make you want to be more inclined to think, okay, there's not much more to do here? Or is that just not a thing? It just depends really on the facts of the incident itself. And maybe these remedial actions taken, don't necessarily weigh on whether or not you're going to get a response back.

Gene Fishel:

Of course, it's fact dependent. It's always going to be fact dependent. However, and this is what I've told companies when I was giving talks as a regulator, the thing that will impress me or lower the temperature, if it's a sensitive breach, is when an organization gives notice early. That will include just in short, the earlier the notice to the AG's office, the better. That's really what companies should take away from this. But I certainly received notifications where maybe the company was not ready or was in the process of assembling the notice that it was going to send out to the affected consumers. But they just gave us a heads up, "Hey, we suffered this breach. I don't have the formal notice ready to send to you or the consumer. But that's in the works. Just letting you know."

I think a lot of regulators are suspicious of obstruction and stonewalling when it comes to incidents. I think the earlier that happens, you're essentially building up goodwill with the regulator. I've just seen it so many different ways that if they're giving off the impression that they're stonewalling or obstructing, it's not going to end well. It's going to cost them more time and money. It's going to raise the ire of the regulators and kind of force them to take a closer look, and maybe even send legal process, subpoenas, orders, whatever it is.

So, I always appreciated that advance notice to the point, and now, being on the other side, of course, and I knew this also at the time, there are many considerations to take in when notifying a regulator. One being if you even have to, but there a lot of other things to shore up, privilege and a lot of considerations. So, assuming you can, assuming it's prudent, I just recommend notice as early as possible.

One thing I'll say just to finish up this point, and one thing I appreciate now representing clients and being on this side is, that when I was a regulator, I really had a singular focus. And, that focus was to get the best results for citizens of Virginia, to ensure that there was restitution, if that was need be, and ensure that organizations were following the law. On this side, representing clients, it's much more complex. There's just so many more things to consider. Their business interests to consider, their privilege issues to consider of course. When we're representing in a regulatory investigation, there's potential multi-district litigation, or class actions that could spawn from the incident. There's even consideration of potential co-defendants in an action.

So, it's a much more complex and challenging practice on this side, which I've liked. And, one thing I like with Troutman, in particular – and I knew Troutman's reputation, that's why I came over here, I knew of it, it enjoys such a great reputation – is just the high level of talent with attorneys and staff and the diverse skill set. And also, and I talked with a lot of partners at the firm, I just love the team approach we take here at Troutman, and working and collaborating with you, Sadia. And when I say high-level talent, I'm referring to and your team.

Sadia Mirza:

That's what I wanted to confirm. I wanted to confirm that I impressed you.

Gene Fishel:

The cross-collaboration and the 360 approach we're taking with you and your incident response team and our investigations team, I think, is serving our clients well. It's just such a unique approach to tackling what is a very complex, or can be a very complex, situation.

Sadia Mirza:

So Gene, to summarize what you just said, it sounds like you think I earned that medal that you're going to send me after this report.

Gene Fishel:

Yes.

Sadia Mirza:

Okay. Good, good. Okay, Gene, I'm really glad that you ended with that, because that was my question. It was going to be now that you're on the other side, is there anything you learned from your time at Troutman that you would have considered? Or you wish you'd have considered more at your time at the AG's office? And it sounds like you've always known that it's a complex issue, and maybe you get more visibility into all the complexities that businesses actually deal with.

Gene Fishel:

Yes, absolutely.

Sadia Mirza:

I will say, your point about notifying early, when doing incident response, I'm always thinking about, at the end of the day, what's the story that I have to tell regulators about the incident? What's the story I'm going to tell consumers? Or, what's the story that the media is going to pick up on? I always think it depends, right? But usually, it's a better story, when you can say, "Look, as soon as we figured you know what was going on. We told you what happened. We told you even before we figured it out, just so it was on your radar." So, that early notification, I do think is very helpful.

Gene, I know I said this is a very important question, mainly for my own personal purposes, because I travel around. I'm always interested in knowing 'favorite restaurant,' your favorite restaurant in Richmond? Stephen, also a member of RISE, a practice leader of RISE, gave me his recommendation while I was out there, but I'm going to be back out there in March. And so, what do I need to try?

Gene Fishel:

Oh, man. That's a tough question. We have a great – Richmond actually has, I think, a very underrated restaurant scene here. We have some great restaurants. Gosh, I would say, one of my favorites, but it's tough to get a reservation, is L'Opossum.

Sadia Mirza:

Okay. That's exactly what Stephen said.

Gene Fishel:

Is it really?

Sadia Mirza:

Yes. It is exactly what he said. So, right now, I'm making a reservation for March.

Gene Fishel:

Yes, you absolutely have to go. It's in a very cool space. It's tough, like I said, it's tough to get a reservation.

Sadia Mirza:

Okay. Here's what I'm doing. I'm making a reservation for you, me, and Stephen. But Gene, thank you so much for joining me. I always learned so much talking to you. It always makes me think about the incidents I have right now and how I could change my approach or what more I could do to kind of minimize, hopefully, any further inquiries from regulators. So, again, thank you for your time. I really appreciate it. Thanks to the audience for tuning in. We'll be back again next month with another episode of *Unauthorized Access*. Thanks so much.