Lowenstein Sandler's Regulatory Compliance & Dispute Resolution podcast: Regulatory Matters

Episode 5 -
Fighting the Constantly Evolving Threat of Cybercrimes

By Kathleen McGee and Elizabeth Roper
April 2022

Kevin Iredell: Welcome to the Lowenstein Sandler podcast series. I'm Kevin Iredell, Chief Marketing Officer at Lowenstein Sandler. Before we begin, please take a moment to subscribe to our podcast series at lowenstein.com/podcasts. Or find us on iTunes, Spotify, Pandora, Google podcast, and SoundCloud. Now let's take a listen.

Kathleen McGee: Hello and welcome to Regulatory Matters, a podcast devoted to covering the ever-changing regulatory landscape affecting business today.

This podcast is hosted by a group of women Partners from the law firm of Lowenstein Sandler, who collectively cover much of that regulatory landscape. We're so glad you've decided to listen and if you have a regulation matters issue you'd like to hear more about, please let us know.

I'm Kathleen McGee and I'm here today with Elizabeth Roper, Chief of the Cybercrime and Identity Theft Bureau at the Manhattan District Attorney's Office in New York City. Liz and her team investigate cybercrime with a global reach and it's no surprise that the cases this bureau chooses to pursue have significance. Liz's leadership is all the more significant because it represents a growing, but still underrepresented force in the fight against cybercrime, women at the helm. This is still a male dominated field. According to a 2019 article in Cybercrime Magazine, women make up 20% of the global cybercrime enforcement workforce. That number is up from 11% in 2013. Assistant District Attorney Roper has seen that growth firsthand, and we get to ask her for her view from the captain's chair today. With that, let's get started. Liz, my friend, welcome.

Elizabeth Roper: Thank you so much, Kathleen. I'm so happy that you and your colleagues are doing this podcast. I'm so flattered that you gave me the opportunity to come on and chat with you.

Kathleen McGee: Oh, my gosh. You're on my short list, I think you're amazing and I love to share accomplishments, especially by women leaders in tech fields. So I'm really, really thrilled that you're here today, thanks.

Let me just kick off by saying, I want the audience to know a bit about your background. Did you envision yourself as a cybercrime expert when you began your legal career?

Elizabeth Roper: Not at all. I'm not sure I see myself as a cybercrime expert right now, it's such a complex, evolving field. But no, I have a liberal arts background. I was an English and French major, no computer science training really whatsoever or anything like that. It's been very much a kind of on the job learning curve for me. And it's not something I would've ever seen as a career to end up in, but I'm so happy that I did.

Kathleen McGee: But your career really has hit its stride during the course of great growth in cybercrime related events, right? Give us a timeline of when you started your career as a prosecutor. And I think listeners, if they know anything will know that that really marches right alongside the trajectory of cybercrime development.

Elizabeth Roper: Yeah. I've been really fortunate in terms of the timing of how this was during my career personally. So I began my legal career here at the Manhattan DA's office in 2006, right out of law school. I started in the division in one of six trial bureaus here at the office and those trial bureaus handle kind of everything, any arrest that comes into the office, whether it's violent crime, property crime, drug related crime, although less and less of that, now, as enforcement of that is shipped a lot. But I always gravitated, even early on to cases that involved a bit more of investigative work. I just found a little bit more engaging than the kind of post-arrest aspects of the job. I think some people love this job because of the courtroom aspect of it and being on trial.

And I always found the kind of pre-arrest stuff piecing together a puzzle and the kind of who done it, of it all to be the most engaging aspect of it. And at that time, in the mid 2000s, the bureau that I oversee now didn't exist. There was this kind of volunteer group of lawyers who did what we collectively referred to as identity theft investigations, kind of now what we would probably call financially motivated cybercrime. But it was kind of this call to describe cases that were probably not large enough for our investigations division bureaus at the time, not major economic crimes cases, not securities fraud, not racketeering, but cases that required a bit more investigative work than really could be done by traditional trial bureau. And at the time, those were really the cases that involved a lot of sophisticated cyber work.

So on third party communications providers, maybe eavesdropping over things like messaging services, international press for data. And part of that is because as you know, so many of the perpetrators of these kinds of crimes, so many of the threat actors are overseas and a lot of them are really quite sophisticated. And they were really early adopters of things like encryption technology, end-to-end encrypted messaging using digital currencies before Crypto was a thing to launder proceeds of criminal activity. And so we just developed a fluency around those issues by virtue of doing those cases. We ended up dealing with a lot of the providers, developing relationships with them, understanding what kinds of legal process were required to get what kinds of data. And now all of those areas of expertise are kind of housed in the bureau that I oversee now.

Kathleen McGee: I love that you have this historical overview, sort of in real time of the development of ... This sounds very lawyeristic, but new ways to commit crime.

Elizabeth Roper: Yeah. That's true.

Kathleen McGee: It is a really interesting perspective to have. So when did you take over the helm of this bureau and in its sort of nascent form?

Elizabeth Roper: So the cybercrime and identity theft bureau was something that Cy Vance created when he became DA when he took office in 2010. I joined the bureau as a line, in, I want to say 2012, although I had, as I said, kind of always been doing a little bit of this work with the leadership of the bureau. In 2014, I became a deputy bureau chief here, and that was kind of my first supervisory role in the office. And then in, I guess it was 2018 when the bureau chief at the time was leaving, took over the helm of the bureau. So it's been, I don't know, three years, three and a half years.

Kathleen McGee: That's fantastic. Can you tell us a little bit about who works at the bureau? You know, people often think it's a bunch of lawyers, but I know your secret sauce is not just lawyers. It's really a staff of committed people.

Elizabeth Roper: Yeah. Thank you so much for asking that and recognizing that. One of my favorite things is getting to talk about my team because they are, they're just awesome. So as you said, it's a dynamic group of people. We have attorneys, obviously, we have about 12 assistant DAs who work in bureau, three of whom are deputy bureau chiefs. We have about the same amount of analysts. So people who are early in their careers, maybe right out of college or graduate school, or a few years in do a lot of the data analysis of the records that we get and help us mostly identify perpetrators of crime, but really help build cases and testify at trial, things like that. We also have a dedicated group of investigators. So people who are traditional kind of law enforcement can do things like make arrests and execute search warrants and take statements from people.

You know, having them here is really, I think, instrumental to our success because we work so hand in hand, it's not, we're not just reactive to an arrest having been made. We all can kind of collaborate and say, what's the outcome we're trying to achieve here. Same thing with the group of NYPD detectives who are housed in our bureau. That's something my predecessor created, a sort of task force with us and the NYPD that allows us to do that kind of work with them as well. So really kind of craft a case from the first day together and decide kind of what's the most impactful path forward. We also have in my bureau, a really unique group of people called the cybercrime intelligence unit, but it's a cool name. They do really, I find it to be really exciting.

They're all foreign language speakers, and they're all kind of subject matter experts in this really niche area of financial motivated cybercrime specifically that kind that is facilitated on elite cybercrime forums that have been around for, in many cases, decades. And so a lot of these targets are really kind of significant in the cybercrime community and the idea behind that work is to develop, again, cases that are going to be impactful. So it might take years to attribute a real world identity to one of these people, and we might not ever be able to arrest them. But the idea is that if we can, that's so much more meaningful, both from a... Both from having any impact in the threat

landscape by sort of removing someone from it. But also in terms of the intelligence that we can get by virtue of talking to people, maybe getting the opportunity to see some of their communications.

Elizabeth Roper: So that's been a really interesting thing to see. And then the last thing I'll mention is my bureau also houses our office's digital forensics lab, which for me, has been one of the most exciting aspects of this job is to get to work so closely with that team. They do the digital forensics work throughout the DA's office. So any device that comes in that we need search, with a search warrant or with consent, they will intake the device and do the analysis of it. So it could be on a homicide case, it could be on a cybercrime case, it could be on a securities case, but they're housed in cyber kind of by virtue of what I was describing before, it sort of organically happened that expertise housed in this bureau because the work that we did so frequently touched on sophisticated cyber techniques. And now we have the opportunity to kind of work hand in hand with them to talk about, innovative investigative strategies and things we can do to kind of demonstrate on cyber cases that might then be impactful on cases throughout the office, ways to kind of get the data that they're seeing about things like encrypted devices. So that team has been really exciting to work with for me.

Kathleen McGee: I mean, you have, I think in all, I've heard you say it before, maybe 60 to 70 people working on your group, is that about right?

Elizabeth Roper: Yeah, that's about right.

Kathleen McGee: It's an amazing workforce. I know you guys do great work and to steal one of your phrases, it is incredibly impactful because you sit at one of the financial centers for the world. So cybercrime, to the extent it touches on financial crime is really a global enterprise. So your jurisdiction is global. Is that right?

Elizabeth Roper: Yeah, that's right. It's, it's funny because we are a local prosecutor's office and geographically speaking Manhattan is tiny. So our jurisdiction in some ways is quite small. The Manhattan DA's office has jurisdiction to prosecute criminal activity that happens in Manhattan. But as you said, Manhattan is a financial center of the world. And so a lot of financial crime touches on some entity in Manhattan at one point a correspondent bank or a company that's been breached or victimized, a company that's being used to launder funds. So we have jurisdiction over a huge percentage of kind of the cyber activity that we see. I do sometimes wish we had more server farms here in Manhattan because getting warrants to search that type of data can be challenging, but yeah, we do take a, we do take an extensive view of it.

Kathleen McGee: Maybe someday servers will be obsolete and you'll have to find another way to grab jurisdiction. Maybe, maybe not too far in the future.

What, what about victims? And I asked this because I think as you started to describe the historical trajectory of the office's movement towards small incidents that occurred online, or that happened to touch the internet or cyber, as we then knew it to now, where there are a lot of varied, sophisticated enterprises, has the notion of who's a victim also changed? And I say this both as a former sex crimes prosecutor myself, who

understood back in my day as a prosecutor, that there was a really limited, but sophisticated interface, especially for trafficking, and some very scurrilous behavior, horrible behavior online. But now, most of my clients are dealing with ransomware as a real event. So you really have this wide variety of victims. Tell me about that.

Elizabeth Roper: Yeah, I think you make such a good point. And I think, you have a really interesting perspective on that as well, as someone who's in private practice dealing with, bigger entities that are being victimized also, with the historical perspective from the prosecutor's chair of seeing all manner of victims across different cases. I guess I would say a couple of things. You and I have both read the sort of statistics about things like ransomware and the shifting victim profiles, increasingly ransomware attacks are targeting massive corporations, municipalities, school districts, huge hospital networks, things like that. Whereas it used to be, in like 2013, 14, we would see people coming in off the street into our office saying, "this ransomware popup, I just got, what do I do?" I think we see that a lot less now because the people who are responsible for ransomware attacks realize kind of where the high value is.

And it's in these massive entities that can't really afford to have their data encrypted for hours or days or week. So I think that's certainly the macro trend. From a local prosecutor's perspective though, I would say we continue see all kinds of victims, and I think that's increasingly true when you have things like the NFT marketplace and these spaces that are really exciting for people, but are also still a little bit opaque and unregulated. And so we see a lot of individual victims, both who are very sophisticated people ranging from really technical people, to people who are pretty new to this space. We see individuals who are victimized by things like business email compromise, as well as huge organizations. So I think the data is consistent with a trend towards bigger and bigger institutional victims, but from where we sit, we're still seeing a mix. It really can be anyone.

Kathleen McGee: I think this next two years I'm projecting my business uptick will be the potential defraud of investors through things like NFTs and other sort of, or claims related to the same. It's going to be a really interesting ride for the next couple of years.

Elizabeth Roper: Yeah.

Kathleen McGee: Along those lines, I did want to ask you, it's a, it's a common risk perception that I'm always fighting with my clients. I know you and I have publicly presented together on this a little bit. And I wanted to give you an opportunity to explain to the audience why they shouldn't be afraid to report things to law enforcement.

Elizabeth Roper: Yeah. Thank you for that opportunity. And it's so refreshing to have a partner on the private side who has your perspective as a former prosecutor and kind of understands the value in working with law enforcement in these scenarios. We have both, right. We have some instances where people come to us and say, I've been the victim of a breach, and that's the best case scenario, right? From the beginning of the investigation, you're working together, sharing information, we're mindful of the victim's interests. They're mindful of what we

need. At times we'll find out about an event like a downstream victim whose PII was used or through some kind of proactive investigation of one of these rooms where the data is being monetized and we'll run into a victim who is not cooperative. And I think you're exactly right, there does seem to be this misperception that law enforcement, whether it's us or the FBI, or the NYPD, the Secret Service, are really just looking to make a case anywhere we can and so if we're not able to attribute the breach to someone, we're going to kind of turn our sights on the victim and see what case we can make there, what wrong is going on.

Kathleen McGee: Cause you have nothing else to do, so

Elizabeth Roper: Exactly.

Kathleen McGee: Right.

Elizabeth Roper: And I think that's exactly right. I think the reality is especially cybercrime space, the resources are such so thin everywhere. We're all just looking to kind of make the best case we can that, and to use a word I keep using, is going to have an impact in the kind of threat world. And so we're really not looking to play a game of gotcha with some victim, who's giving us information because that's just completely counter to our objectives. We're trying to trust we're to protect the community and to say kind of, "all right, now, we're going to try to kind of generate some approval case against the victim for mishandling data or whatever we can find underneath the hood" is just in anyone's interests. That's not to say we won't follow the evidence where it takes us and if there's something glaringly criminal going on we won't, we won't turn a blind eye that, but that's never our objective. It's never objective to go in to a meeting with a victim or a conversation with a victim and say, what were you really doing here? You know, what was going on?

Kathleen McGee: Right. I hope that's a good take. I hope it's a takeaway our listeners really hold on to. I wanted to actually pivot just a little bit. You heard me at the beginning of the podcast talk about what I think are really unsurprising statistics about the lower, but growing representation of women in cybercrime enforcement globally. And I want to ask you whether or not you think that there are particular challenges or even opportunities for women in this field and are you encouraging growth?

Elizabeth Roper: Yeah. I think that's such an important question. And I think there's both, right. There's challenges that we're all familiar with and also some really exciting opportunities. I think challenges because even more so than in other fields, there's a perception here that women aren't as competent when it comes to computer science and data analysis and the like, but I also think because so many aspects of this space are new. There may be a little bit less tethered to some of the traditional hierarchies you see in other fields. Crypto is obviously the example here where you see a lot of really impressive women leaders in this space, GCs, CEOs, journalists, who are really dominant in that field. And that's really exciting to see. And I think and hope we'll continue to see more of that in the kind of innovation space going forward. But of course there are always going to be challenges.

Kathleen McGee: Yeah. I think though highlighting, and I think it's important for listeners, especially younger council who might be listening to this podcast to really understand that opportunities... you can find these opportunities. You did. And especially in a growing area like this they're exciting and novel and they have people like you to look up to a little bit. Dare I say.

Elizabeth Roper: And like you.

Kathleen McGee: Let me ask you, you know this, it was coming to this. I mentioned to you when I was talking up the podcast that we do tend to ask our guests about a fun fact. Tell me your fun fact, something that we might not know about you, but that you're willing to share.

Elizabeth Roper: Yeah. So I did give this a lot of thought. It's tough. I don't know.

Kathleen McGee: I know, it always is, right? You're like, what's fun about me? Oh, maybe that would be fun.

Elizabeth Roper: Right. One of the things that came to mind is... I think we've all developed quirks during the past couple of years of quarantine and weird hobbies, whether people are making sourdough, crocheting, or whatever. And one of the things that I really became fond of doing is biking my kids around the city, in this car bike that my family acquired. So it's like a huge bucket in the back of this bike where my kids can sit. And sometimes even our dog and we'll bike to Washington Heights or to Prospect Park, we've taken it on the ferries. We've taken it to museums. And it's just been an amazing way to kind of get out of the house and get around the city. So if your listeners see us riding around with a couple of young kids in the back of a bike, please wave and say hello.

Kathleen McGee: I love it. Although I will ask, can you fit in there? Can someone else ride you around in the box, in the back? Just so that you have that perspective. I mean, it must be amazing for them.

Elizabeth Roper: Yeah. So apparently the weight capacity of this bucket is like 600 pounds. So I have gotten in it. I like, I like the view from the front better than sitting in the bucket, but it is possible.

Kathleen McGee: I love it. That is a... That is fun and a fun fact. Perfect. Well, thank you so much, Liz. I've really valued the conversation. I'm sure our listeners are going to find it really interesting. Thank you so much for joining today.

Elizabeth Roper: Thank you so much for having me, Kathleen. It was so great to chat with you.

Kathleen McGee: My pleasure. Yeah, I'll see you soon.

Elizabeth Roper: I hope so.

Kevin Iredell: Thank you for listening to today's episode. Please subscribe to our podcast series at lowenstein.com/podcasts, or find us on iTunes, Spotify, Pandora, Google podcasts, and SoundCloud. Lowenstein Sandler podcast series is