CRYPTO EXCHANGE, S02 EP01, EVALUATING FRAUD UNDER THE BANK SECRECY ACT
RECORDED DECEMBER 2022
HOST: CARLIN MCCRORY
GUEST: TERRI SANDS, MANAGING DIRECTOR – DISPUTES, COMPLIANCE, AND INVESTIGATIONS, STOUT

Carlin McCrory:

Welcome to another episode of the *Crypto Exchange*, a Troutman Pepper podcast focusing on the world of digital assets and payments. As longtime leaders in the intersecting worlds of law, business, and government regulations, our lawyers can go beyond the buzzwords and headlines to make sense of the emerging legal and regulatory frameworks for operating in the digital asset and payments industries.

I'm Carlin McCrory, one of the hosts of the podcast and an attorney at Troutman Pepper. Before we jump into today's episode, let me remind you to visit and subscribe to our blog, consumerfinancialserviceslawmonitor.com. And don't forget to check out our other podcast on troutman.com/podcast. We have episodes that focus on trends that drive enforcement activity, consumer financial services, the Fair Credit Reporting Act, cybersecurity, hot-button labor and employment law issues, and more. Make sure to subscribe to hear the latest episodes.

Today, I'm joined by Terri Sands from Stout to discuss the risks and regulatory scrutiny that financial institutions face related to fraud in the Bank Secrecy Act. Stout is a global investment bank and advisory firm specializing in corporate finance, transaction advisory, valuation, financial disputes, claims, and investigations. Terri, who is the managing director of the Disputes, Compliance, and Investigations Group at Stout, specializes in payments and regulatory compliance and financial crimes. Terri has extensive experience in the financial services industry, including 20 years of consulting experience and 15 years of direct banking experience including the Federal Reserve Bank of Atlanta and serving in various positions in a community bank including director of payment strategy and risk management and director of financial investigations unit. Throughout her career, Terri has served as a leader in the payments, BSA/AML and OFAC/Sanctions, and fraud and risk management areas providing education, risk management, strategy, compliance, and program enhancement support for financial institutions of all types and sizes including FinTech providers. I'm so thrilled that we can have Terri on the podcast today and I'm looking forward to the discussion today. We'll dive right in.

Terri, what do you see as the biggest risk that financial institutions face today in the areas of fraud and BSA?

Terri Sands:

This is generally just working in the financial industry and we see the evolving risk in the fraud in the BSA area. And so, one of the biggest things is we see people just not being prepared — people not being trained, not a focus on training, not a focus on understanding how bad fraud is out there and understanding the money laundering risk out there. And I think we see more of that today than ever before. It's scary. In the world in which we live in and the fraud that's out

there and the money laundering risk that's out there that some financial institutions, they just don't get it in terms of making sure that they're people trained.

The other thing that I think that we see a lot of is truly the lack of structure. And I think in the good old days when we didn't have to worry about as much fraud and as much money laundering risk and before 9/11 hit, people were used to doing more manual processes and they had more time. I think today you have to have that lack of structure because if you have fraud, you have only so much time to respond to it. If you see something suspicious, you have only so much time. So everything's so deadline-oriented today just because fraud happens fast. And to submit a suspicious activity report, you have 30 days from the identification of the suspicious activity. So I think everything is so deadline-oriented and so fast that the lack of organizational structure really hurts a lot of financial institutions and FinTech companies. So just not being prepared.

I would also say that we see when we go into financial institutions. And we do a lot of postmortem fraud reviews to really outline for a financial institution what went wrong, what you could have done, and what are the gaps in your process now. And what we see is multiple lines of first line of defense, second line of defense, third line of defense — multiple lines of people just not knowing what to do and there's no organizational structure to set the parameters of, "These are the things that you need to do." And we see that a lot. So I think probably the third part of that is there's no organizational discipline. And you can't have that today in the world in which we live in with all of these external fraud threats. And we see this in all the disaster events that are going on.

I think the last part of that question is really not an understanding for the effectiveness of their own fraud and BSA systems. We go in and we do a lot of work optimizing fraud systems/optimizing AML systems because we see there's all of these alerts that are unproductive – a lot of these false positive alerts. So, in a normal day, what you find is that people who are responsible for the day-to-day (the fraud alerts and the AML alerts), they're spending so much of their time working those false alerts that they're not focused. Their system's producing thousands of alerts that are false positive, so they're really missing the positive alerts. And so, it's so important to make sure that your systems are optimized and they're working for you — not living in this "manual spreadsheets / working out of the system / false positives / not really having the effectiveness of the system." So, we see that truly as the biggest risk — not aligning your people and systems with the times, all the external fraud threats, disaster events, and all of the money laundering threats that we have today.

Carlin McCrory:

That's really interesting, Terri. Three of your four points mentioned the people involved in all of this and maybe a lack of training or experience, or maybe they're overwhelmed with the amount of alerts coming in. Are there any general recommendations that you have for our listeners?

Terri Sands:

One of the things that we constantly stress to our financial institutions and FinTech companies? Look, if your strategy is to grow your business whether that's through acquisitions, you buying other banks or credit unions, or credit union buying a bank, or just through organic growth, if your strategic plan is to grow, you have to grow your risk management with that. We do see

that. The people stay static, but the bank or the FinTech company is growing. And I think it's just people doing the same thing that they've done 10 years ago and staying in that static position without growing with the strategy of the bank, the credit union, or the FinTech company. You get into this bad situation where you just end up not being sustainable and you can't keep up. And so, we stress that. If you're going to grow, make sure that your risk management practices align with your growth.

Carlin McCrory:

Well, that makes a lot of sense. And that dovetails into the next question that I wanted to ask you, which is: what in your opinion or the main reasons that financial institutions find themselves under regulatory scrutiny?

Terri Sands:

One of the things that we've seen over the past two years is that financial institutions simply don't have the resources. Either people have left retired. You have the BSA officer who's been there for 30 years – all of the history, all of the knowledge leaves, no succession plan, no idea about the number of staff you are supposed to have to carry out your BSA and quite frankly, your fraud program. But really the resources. One of the things that we see is very damaging for a financial institution is first not having a succession plan for these key positions. It's just a bad idea.

The second thing is not having a staffing assessment of your AML program or even your fraud program. Just kind of going through the day-to-day, and everybody's super busy so everybody kind of goes through their day-to-day without taking a step back and going, "Wait a second, do we have enough staff?" So when examiners come in there, they're going to look at all of the work that you have, all of the high risk clients that you have, they're going to look at where you are geographically, where your footprint is, and they're going to start adding up all of the things you're doing and they're going to say, "Hey, you've run out of time. You don't have enough staff to carry out what you're doing." That in itself starts pulling the string on, "Is your internal controls effective? What about your BSA officer?" So it starts pulling the strings there, and we do see the resources. And again, just over the past couple of years, I will say it has been significant.

And quite frankly, if you think about the world in which we live in and all the risks that are going out there, there are BSA officers today — and we see this, we've seen this over the past couple of years — who simply just can't do it. They do not want the stress. They walk out and then a financial institution is left to go, "Now what? What do we do now?" Definitely resources is one thing.

And the other thing that we see is where financial institution will be banking high risk clients, but they won't add the staff or the expertise that they need in order to bank those high risk. So again, it kind of goes back to what I was saying about being static. Your strategic initiative is to grow the business. Bank higher risk clients — they're more profitable, but yet your staffing model stays the same. You don't have the right experience, so that stays static. And again, these things don't align. So when examiners come in, or quite frankly when external auditors come in and they look at the program, they're like, "How are you keeping up with that?" We do see a lot of that today.

Carlin McCrory:

It's up to executive management and the board to make sure you're fully staffed and adequately prepared and everything like that. So what do you see from the executive management in the board to prepare for some of these external fraud threats and BSA risks beyond just making sure you're properly staffed?

Terri Sands:

That goes back to what do we see as where financial institutions get themselves into regulatory scrutiny. Sometimes we see where executive management and the board, they have a culture of compliance. They understand it. They get it. The board of directors gets the fact that they can be personally held liable if something happens. They understand their oversight role of that BSA program.

On the other hand, and this kind of goes back to the regulatory scrutiny, when we see a board of directors going in and just approving everything. "Here's comes the BSA program, I'm going to approve." The BSA officer reports up to the board going, "We have enough staff. I approve." If they don't challenge that, "Show me that we do have the appropriate staffing level to carry on what we're doing," and they're not asking questions, what you get is a big gap between what the board thinks they have and what is actually happening until an examiner comes in one day and says, "What's going on here?"

The good news is that we do see today more and more boards of directors really take in an active role because executive management is going to them going, "We've got to have the board being more active in this role." But then when we help financial institutions out of regulatory orders, we still see that big gap between, again, what the board thinks is going on and what is actually going on. Simply because in the day-to-day world in the real life, if a BSA officer and their support staff is sitting there every day and no one's raising their hand and going, "Wait a second, we don't have the staff to carry out," and they're just trying to get through the day, that never gets escalated to executive management and it doesn't get escalated to the board, then that's where you have the big ginormous gap between what the board thinks is going on and what is actually happening day-to-day.

Carlin McCrory:

Right. And you need to make sure, I suppose, that BSA officer is telling executive management, "Hey, we need more folks," or "We need these resources," or something like that.

Terri Sands:

Right.

Carlin McCrory:

In discussing this, do you find that financial institutions have started to put more of an emphasis on their BSA and fraud programs? You talked a lot about the structural programs from the past and how we need to be more loose and how things have been changing and evolving and we can't keep up with the fraud almost. It's so vast. What have you seen that the financial institutions are doing in this space?

Terri Sands:

I think COVID-19 woke up a lot of financial institutions because they were changing the way that they did business. They were also finding in that disaster event where everybody was trying to figure out what to do at the same time that fraud hit significantly.

One of the things that we do see and that we hear from our clients is they're drowning in fraud. Right now, with more and more financial institutions, executive management are taking that active role in, "What does our fraud program look like? What does our BSA program look like?" And we have done more strategic enhancement projects over the past couple of years than ever, just because if you've been hit with a significant fraud event, and we've had small financial institutions get hit with millions of dollars in wire fraud, hundreds of thousand dollars in check fraud, debit card fraud, it is so significant that one event will change the way that a financial institution does business.

And so, what we are seeing is probably 99% of the time financial institutions that have had a significant fraud event come out or regulatory scrutiny, they basically change the entire way that they do business. So, they actually put forth the effort to then do a risk management strategy where they're looking at all these gaps and looking at all these things. The unfortunate piece about that in what we see is that too many financial institutions wait till that point where they're upside down and they're just trying to figure out how to get out of that fraud event that they're in before they can get to the point that it becomes a strategy.

I always say this to financial institutions: "Look, if you're not in the middle of a fraud event or a regulatory criticism, if you're not in the middle of that, you have all of these options. If you are in the middle of a significant fraud event, you're just trying to work yourself out of it or regulatory scrutiny, you only have so many options."

And so what we try to do with our financial institutions and quite frankly, FinTech companies, is really stress the fact that to be strategic in the world in which we live in now is so incredibly important because if you're in a middle of a fraud event, you can't really figure out who's doing what. You're trying to figure out who's doing what while trying to figure out how you're going to recover funds everything at once. It needs to be such that there's organizational discipline and structure so you prepare everybody. If you have a fraud event or if you suspect fraud: "Here's a direct path for escalation. This is what you do." The "one, two, threes" rather than people running around the building on the phone screaming and going, "What do I do?" That's not the way to handle it.

So, the strategic piece of that has become very important. The unfortunate part of that, like I said, is that what we see more than not is financial institutions and FinTech companies waiting until they're in the middle of a bad situation in order to change the way that they do business.

Carlin McCrory:

Yeah, that's scramble. It's never a good thing, right? I do want to dive into the payment side of things as it relates to fraud. We've done a prior episode on P2P fraud. And honestly, a lot has changed even since then. So, we'll first dive into P2P fraud and just get your thoughts on that. What are you seeing? How are the financial institutions handling it? Any recommendations? Just your general thoughts.

Terri Sands:

Person-to-person fraud is one of those things that we talk about probably four to five times a day. It's one of the things I'll wake up probably thinking about P2P fraud and go to bed thinking about P2P fraud. The general consensus from our clients is, "We don't know how to do this anymore."

Like I said, in the good old days you had a couple of debit card disputes. You worked the disputes. You did the stuff. I think in the good old days, we didn't have that mobile device. No one really planned 20 years ago that you would have the ability to load your debit card on all of these different sites, Venmo, or Cash App. All of those things obviously being new, people adding their debit card, in addition to that, not anticipating the fraud threats. Not anticipating all of these fraudsters out there socially engineering people, competence tricking them into, whether that be a 25-year old or a 90-year old, competence tricking them into signing up for Cash App, signing up for Venmo, doing these things, tricking them to move money. We just didn't have that back then. And here we are today with that piece of it. So technology is forced a different way of doing business.

In addition to that, with Reg E out there kind of hovering over everybody's head, really not knowing what's going to happen there. Financial institutions, even as recent as a couple of years ago, if one of their consumers said, "I didn't authorize this. I didn't provide my debit card, didn't do that," that was a regular dispute. So I know how to do, I'll investigate that. It's fine. Even if I have to write that off, it's fine. But with authorized fraud, where our financial institutions are struggling in a big way is the psychology of it. How are you supposed to make people act differently, do something differently, not surrender their debit card information, not fall for all of these different scams? Because there's so many scams out there. How does a financial institution survive? How do they say, "This is a scam. Don't fall for it," when there's thousands of scams?

So it's all of the psychology. How do you get into somebody's brain and say, "Don't do this. Don't move forward." And I think where our financial institutions struggle, and we have this conversation every single day, is we're bleeding money because when we hand that debit card over, we know for a fact that we're going to lose because whether it was, "I gave my debit card information and it was authorized fraud. I actually gave it. I fell for this," it's hard psychologically for a financial institution to understand, "I will take the loss for something someone knowingly did." And I think it's one of those things that we talk about. We've had a big conversation about it just yesterday with our financial institutions and the overall consensus is, "What do we do? What's next with Reg E? And how is that going to impact our bottom line?"

Interesting enough about that is for the first time in years — in years, I've heard it just one other time — for the first time in a long time I guess, financial institutions are starting to really strategically figure out, "Do I offer a debit card? Do I offer Zelle?" And again, FedNow's coming out. Real-Time Payments is here. Do we get further down the road? Do we offer all of these different P2P services knowing that we are going to be on the hook for authorized fraud? I think it's a struggle.

In my opinion, only in my opinion, I think that this is really going to be more of a strategy on, "Do we offer these services knowing that we're going to take the hit on them?" And I think you're going to start seeing something that you've probably never seen before where financial institutions before would just offer things like Zelle and person-to-person payments, whether it's

Real-Time Payments or whether that's FedNow. I think we are in a position, I'm hearing, with financial institutions taking a very long pause and figuring it out. That's just where we are today. We just don't know.

Carlin McCrory:

You mentioned RTP, Real-Time Payments, and FedNow, which will be coming we think this spring of '23. Do you see that being a longer pause for adoption? Or at least on the consumer side, more precautions are being taken because of the fraud that we're seeing?

Terri Sands:

We're having conversations with our member financial institutions, and we're talking more and more about, "What are you thinking? Going into this, knowing all of this Reg E stuff, knowing that it is a risk, what are you going to do?" And I will tell you, not just on the consumer side but also on the commercial side with Real-Time Payments and FedNow, it is a pause because I think what we are hearing is, "Two years ago, we were excited. Now we are going to wait and see." And that's just talking to our financial institutions.

And quite frankly, it's no different than anything else. We saw this years ago with remote deposit capture back in 2009. We've seen this before where financial institutions are sitting back and going, "We want all of you other financial institutions to go out there, experience the fraud, experience what this is going to do, and come back to us and then we're going to decide strategically if we're going to move forward." But I'm just not... And it's unfortunate because I think Real-Time Payments and FedNow, I love that that's happening. I love the fact that you could have different options for moving payments. I think that's a great thing. It's not to discount those services, but financial institutions find themselves in a really sticky situation right now trying to decide, "Do we do this or not?" Regulatory environments change. Like I said, Reg E, what's going to happen? They're bleeding money on authorized fraud today just with what they have in Cash App, Zelle, Venmo, those P2P options today. And it's just one more thing.

And we talked to executive management and board of directors about this too, where they'll ask us to come in and do a presentation. One of the things that we're finding is a board member or executive management's going, "What's the benefit to jump in it immediately? What are we going to miss?" because it's not like consumers and businesses are begging for it now. To me, in talking to financial institutions we serve, it's more of a, it's not that they're not going to do it. But I got to tell you, people are taking more of a, "Let's pause and step back and make this more strategic" rather than what they used to do and say, "Oh, there's a new payment collection system. We're going to pop right in there and offer it. As soon as you walk in the door, that's what we're going to do." And it is, again, just with the external fraud threats and the things that are happening within their own four walls every single day. They have this knowledge every single day. So that's what we're seeing today and hearing from our banks.

Carlin McCrory:

I know we've mentioned a lot about fraud and risks. Do you want to just hit on the highlights again of the things that our financial institutions and FinTechs can do to be prepared and be proactive before we culminate the episode?

Terri Sands:

I think that organizational structure and discipline are going to be important. Fraud is a business. It is a business. These fraudsters out there, they're very structured. They've got organizational discipline. They've got organizational structure where financial institutions are going to fail if they don't have the same thing. You've got to fight the bite now. And so that organizational structure and discipline becomes so incredibly important just because of all the social engineering exercises and the phishing and all of the scams that go on. I also think that systems are going to be important. Financial institutions for years don't know how their systems work and sit there and have really terrible systems. They'll work outside of the system or they'll start hiring more staff to work in this crappy system. So they also need to understand, "Your systems need to work." Technology is important because again, on the fraudster side of the house, they've got the technology too. Financial institutions who do not understand and really truly understand the effectiveness of their systems, it's going to not be good.

And then, like we talked about, people. You need to have succession planning and a staffing assessment, because we do see and we hear financial institutions over the past several years saying, "This person will never leave," but that person leaves. You can't plan on someone staying forever. You always have to have a succession and equally as important, to make sure that you have enough people to carry out your program. Because if you don't know that and an examiner comes in and tells you that, that starts pulling the string on the effectiveness of your overall AML, and quite frankly, your fraud system.

Carlin McCrory:

All right. Well, Terri, thank you so much for joining us today. We really appreciate your time. And thank you to our audience for listening to today's episode. Don't forget to visit our blog, consumerfinancialserviceslawmonitor.com, and subscribe so you can get the latest updates. Please make sure to also subscribe to this podcast via Apple Podcasts, Google Play, Stitcher, or whatever platform you choose. We look forward to next time. Thank you.