

Episode 63

Trust No One

Intro

This is Risk on Air by Lawcover, and today's episode is about keeping your trust account safe.

Julian: Welcome to Risk on Air. I'm Julian Morrow, and today's episode has the potentially chilling title of Trust No One because it's all about keeping your trust account safe.

And our guest is none other than the Chief Trust Account Investigator for the Law Society of New South Wales, Sharon Blake. You might have read Sharon in the Law Society Journal, there was an article back in February about an investment scam warning to trust account holders, and Sharon's here to tell us all about trust accounts and keeping them safe today.

Welcome, Sharon.

Sharon: Thank you very much.

Julian: Now, Chief Trust Account Investigator, what does that involve?

Sharon: So I'm the head of the Trust Accounts Department. Law practices across New South Wales have obligations under uniform law, and my role is to ensure that they comply with those obligations when it comes to handling trust money and trust accounts.

So, along with my team, we look after a variety of things: investigation into trust account irregularities and anomalies; we accredit external examiners; we accredit trust accounting software to ensure it actually meets the requirements; we receive annual submissions from law practices where they submit their annual Part A and Part B, and these are obligations that apply to all law practices across New South Wales.

We answer a variety of queries from trust accounting support, how do I fix this bank reconciliation, to how do I open a trust account? Not surprisingly, people have a variety of issues with all the different banks and branches that exist across New South Wales, so it's never a quiet moment.

And then in our spare time, we're helping practitioners who've actually got issues with cyber fraud and cybercrime. There's some pretty dodgy scammers and fraudsters out there who are always looking for ways into law practices, and so we do a lot of support and help with those.

Julian: Yeah, so how long have you been in the role and how much has it changed over the time that you've been doing this job?

Sharon: Yes, I've been in this role for about three years now, coming up probably close to four.

But what I've seen is a significant increase in the number of reported cyber incidents, cyber fraud. What we're seeing is that the basics don't change.

Sharon: Scammers, all they ever want to do is get your money, get your data that they can translate to money, transfer to money. But what they're doing is getting a bit more clever at how they're accessing accounts. They're getting clever in how they're manipulating the scripts so that law practices and practitioners are falling for these scams.

Previously, everyone would be aware of the Nigerian prince scam, and everyone's, oh, I would never fall for that. What we're hearing now is fraudsters will ring up and say, "Hi, I'm calling from the bank fraud team." And they go, "Oh, yes, yes, I'm with that bank." People don't stop to think, why would the fraud team be ringing me? Now, the busiest time of the day, at month end, at year end, but they stop and they go, it's the fraud team from my bank. Then this person on the phone pretending to be the fraud team from the bank will build a rapport and a trust. And this is where people unintentionally and unwittingly fall victim to these scams. So what we're seeing is a lot more scam activity in building a profile of law practices. We've seen some of the scripts that come out of some of the compounds where the police have actually raided the fraudsters' scam compounds. And what it shows us is that they've got a variety of tools and a variety of scripts that they use for different scenarios. They've got ones for small law practices, medium law practices, and larger law practices. So what they do is profile law practices here in Australia and break them into cohorts, into buckets, and target them specifically. So what they'll do is they'll look to see, has this law practice got an out of office on? Or has this principal in this practice got an out of office on? Then they'll look at the out of office and they'll see you're out on leave from this date to that date - "All my urgent escalations or queries should go to this person," cool, but a new name, "and all other regular queries should go to this person." So now they've got three contact points, email addresses, phone numbers, and I've got really valuable intel here when I ring up this law practice. So a phone call through to the reception, the fraudster will be able to say "Hi, I was trying to get so and so, but I know he is on holidays or he's in a conference this week" and the person on the phone will assume there is a relationship there because they have all of this information. 'Now I know I'm supposed to refer to so and so but can you pass me to this other person, who I understand will be able to assist me". So that builds a rapport and a trust.

So when emails come in from people they think are sending them (the original senders), they assume that information in that email is safe. So if you've got a potential client sending you through documents and they have already rang and they have said "I'm sending this through, I'll attach the documents" when people have already had the phone call conversation they don't think could this be a fraud, could this be a scam, could it be someone trying to impersonate someone? So what happens then is they click on the link, they open the attachment, malware is loaded onto their device. Now people don't necessarily know what malware is - it doesn't pop up in your screen going, "Hello, malware has landed." It sits in the background.

And what happens is the fraudsters and the scam artists gain intel. They monitor your inbox. They see what traffic is coming through. What kind of practice do you deal with? What kind of matters are you dealing with? What kind of money are you expecting to receive? Yeah, so what they will do is they will use that information they gather to build that profile and see what's the best way to target this specific law practice. So one example we had recently was a law practice had an elderly lady client and she was in her 70s. And she was well known to all members of the law practice.

Sharon: She would come in person, she would talk on the phone, and she had various medical ailments. She would talk about her bunions, she'd talk about the weather, and she'd have a lot of general issues with life.

So on a Thursday afternoon, when the law practice reception receives a phone call from her, they weren't surprised. And then she went into her usual complaining about the weather, talking about an upcoming doctor's visit, but she needed to speak to the finance team because the money that she's just received from selling her house, her family home, has landed in the trust account and she wants to get it before the weekend and she's very excited. Now there was no flags.

So she was put through to the finance manager and the finance manager said, "Oh, we're just in the middle of year end, very, very busy. How can I help you?" "Well, look, I'm going to the doctor this afternoon. I won't be available. But I just want to confirm where you're going to pay the money for my sale to." So the finance manager was distracted by year end. "Yeah, that's fine. Just give me the account details", wrote down the account details, the BSB, the account number. "Yeah, that's fine. Yeah, we'll pay that today. No problem." It got paid out Thursday afternoon. Friday came and went. Saturday came and went. Sunday came and went. And then Monday morning into law practice came the lady with her daughter. "We're here to get the money." And everyone said, "What money?" "We spoke to you on Thursday". "That wasn't me." So her voice had been impersonated. Now, she had been subject to a romance scam previously, so her voice had been used online and the impersonator had been profiling her and had also been able to interact with the law practice pretending to be her.

Julian: Wow. It really shows you how sophisticated these scams are and how one scam can lead to another. It's all the elements of familiarity that can actually become a point of vulnerability.

Sharon: It is. If you were to talk to anyone, they'd say, "Well obviously we will always confirm details."

What happened in this scenario was that the client rang in with the bank details and no one tweaked.

It has to be us ringing out. We've clarified with everybody to make sure that when you're confirming bank details, you make the phone call out to a number that you know, not the number that's on the email, because invariably that will be the fraudster's direct number.

Julian: Well, it sounds like there is never a dull moment when you're the Chief Trust Account Investigator, Sharon.

Now, if we were to step back and look at the big picture in terms of when things go wrong in managing trust accounts, what would you say are the common patterns you've seen?

Sharon: So I've probably seen about more than half relate to business email compromise. Microsoft accounts being compromised, email accounts, Gmail accounts, and online accounts that just don't have secure passwords in place.

I think one of the challenges is people think passwords, how can I remember all of the different passwords for every single website and they have a really bad habit of reusing passwords. That's really, really bad practice. It's the equivalent of walking away and leaving your key in the front door.

Julian: I think I've seen some of your presentations where you describe how quickly passwords can be hacked. I mean is basically instantaneous these days.

Sharon: Pretty much instantaneous and we always recommend at least 12 to 15 characters using a combination of letters, numbers, uppercase and lowercase. Some people use paragraphs, lyrics, or quotes from poems. But I will always hasten to add that there was a fraudster recently who was profiling a practitioner and he accessed their Spotify account. And he saw that on Spotify he had a playlist. He played this playlist pretty regularly and routinely had a favourite song.

The practitioner had actually used the first sentence out of one of the favourite Pink Floyd songs as his password, thinking it was long, more than 20 characters, nobody is going to crack this.

Just be aware that fraudsters have access to everything, your Facebook account, your online activity, when you post photographs outside court, when you publish any documents, any articles. Everything is a piece of information, a breadcrumb, a trail of information that a fraudster can use to build a profile to know you better than you know yourself.

Julian: So it seems like the most common vulnerability is habit or just letting your guard down momentarily. Let's talk then about typical weaknesses and how to avoid them.

Sharon: Probably the biggest one is when people are stressed and busy and life takes over – that human element.

Every single practitioner I talk to who has been subject to a cyber incident has always said to me, "I knew I shouldn't have given anyone my PIN. I knew I shouldn't have clicked on a link."

But in that moment I was waiting for a doctor's call back, I had a whole host of other family dramas, court deadlines, frustrated, angry clients on the phone. There was a whole world happening and in that split second when I got a phone call from a fraudster pretending to be a member of my bank's fraud team, I didn't stop to think.

So it's that pause. When you get an urgent phone call from the bank's fraud team, pause. Take a deep breath, because in that split second, you can save yourself so much time and energy by going pause and pick up your bank card out of your pocket. Say, what's the number on the back of it? Ring that number and say, I've just had a phone call from you, my bank. Can you put me through to the relevant fraud team? Any fraud team that will ever ring you will have no problem with you ringing them back. Fraudsters will. Fraudsters get quite angry on the phone if you say, I'll ring you back on the number I know I should ring you back on. They go, no, why? It's big money. It's gone out of your account. They put pressure. They'll put a real sense of urgency around it. If you don't act now, all this money is going to disappear. Again, in that moment, pause, take a deep breath.

Julian: In terms of tech fixes, multi-factor authentication is obviously important?

Sharon: We know that online there's been a series of data breaches. Companies around the world, email addresses around the world, you know, on any dark web you can find any variety of information. And some people might have already seen there's a white hat hacker from Microsoft has actually produced a database of all the email addresses that have been released to the dark web and the passwords.

Sharon: So even if you just search in there to see has my email been compromised? So if you find your email has been compromised and it happens, right? It happens. Take a deep breath, change your password, set up multi-factor authentication because it's so easy to guess a password and what they often find too is people don't change their passwords significantly. So if your IT team sends you a reminder, say password 123, and you get the email in six weeks, go to change your password, and you go, okay, password 456, and then you get the reminder again, change your password and change it to password 789, what happens is fraudsters can see this pattern. I guess, based on the time of where we are now, their password is going to be either password 10, 11, 12, or 13, 14, 15. So that's a really easy way for hackers to get access.

But if you have multi-factor authentication set up, they might get in the first stage, but they won't be able to get in the second stage, which is where the code comes in. So have multi-factor authentication set up. A lot of users will have it through their Microsoft Office products, through their online banking, but look to set it up for their laptops, their data, anything accessing the law practice information, and just in their personal lives as well.

Julian: What about using shared profiles amongst practitioners in a firm? What risks does that create?

Sharon: So we do see a lot of instances when I walk into a law practice and we see a whiteboard on the wall and they have the username and password, and everyone knows what it is. Or post-it notes with a username and password stuck on a computer. It's the worst practice because invariably it'll get into the wrong hands. So you should have a unique password, a unique user login for every single device. But it's also from a point of view of data and who needs to access what. So from a trust account perspective, not everyone needs to access everything. So that role, responsibility and who has got access to what is very important when you are setting up accounts and profiles.

Julian: What are the risks that come with the use of personal devices?

Sharon: Well, one of the key uses I find is people aren't backing up their data and they don't know how to ensure all their software is up to date. So I often run trial sessions with my own team to see "Have you all with your work laptops or work mobiles checked and seen is all the software up to date"? And invariably people will say, 'Oh, I've no idea how to do that'. So I think one of the first things is if you have a device, laptop, mobile phone, personal mobile phone, work mobile phone, check. Now, is this up to date? And if you don't know, ask your IT team. "How would I know if this is up to date"? "How do I know my software is protected"? And the other thing I often say to practitioners is to... because there's a real reliance now on software, particularly trust accounting software, it's all up in the cloud. So I say to people, like a fire drill, we all do a fire drill, make sure we can all get out of a building in an orderly fashion in the event of a fire. Do the similar thing for a cyber incident.

What happens if your system is compromised and you can't get access to your data? We did have a recent example where a practitioner did have their systems compromised and the fraudster had gotten into the system and said, I've got access to all your data. So the practitioner, so they took a hammer out and start banging their laptop and they got great sense of relief. I've stopped them from accessing my information. They went down to JB Hi-Fi, got another laptop, plugged it into the network.

- Sharon:** The problem doesn't go away because they access the system and the system is up in the cloud. So it's to really understand the device you're using is a physical product, but it's connected to what? Where is your information stored? Where is it backed up? Who are the companies that are providing all those services to you? And if you don't know, ask. Ask your IT team. Ask whoever's providing you support because they're the questions. And there's no such thing as a silly question when it comes to cyber, it's so important that you're aware of where is my information being housed? How is it being backed up? How can I access it in the event of a cyber incident?
- Julian:** Obviously, the critical moments are when money is transferred. What would your advice be in terms of procedures for verifying instructions?
- Sharon:** So the most important thing is to verify the bank account details, but obviously you need to make that phone call out to a trusted number. But we'd always recommend that at the beginning, there's that openness with clients because oftentimes clients aren't as aware of the cyber environment and the threats that exist. And they will trust an email that they get that purports to be coming from a lawyer and they'll always rely on it. We've had so many instances of people that said, but I got an email from you, Mr Lawyer, Mrs Lawyer, to say put the money into this account. Now I knew it wasn't the trust account, but I'm not going to challenge you, you're the lawyer. So by having the conversation at the beginning, you're setting the groundwork that I will always do this. They will never change. They'll at least then have in their memory bank that the lawyer taught me this. I know this is a fraudster. And it's just building that awareness. The harder we make it for the fraudsters, the better.
- Julian:** Staff training then is going to be critical?
- Sharon:** It's really important for people to be, I suppose, in a culture where it's okay to ask questions. So we had an incident before Christmas where the managing partner's email his Outlook had been compromised and emails were sent to the finance team ordering them to make payments out of the trust accounts for upcoming matters that were due for settlement. This wouldn't have been unusual, but he was on leave. So they facilitated out the first payment, then the second payment, then the third payment. We were close to \$6 million at this stage. Then someone got a call from the bank just to say there was an error in one of the account numbers. Can you just confirm it? Now, in this law practice, there wasn't an open culture where the staff felt comfortable to challenge or ask a question of a managing partner. So one of the things we would always say is, particularly in the larger firms, is ensure staff feel it's okay to ask you, is this email from you? We've all seen a lot of the emails and text messages going, pay this now urgently. And people laugh and they say, obviously there's errors in that email I'd never fall for that. But when it comes from a senior member of the leadership team, do the staff feel comfortable to challenge that and just say, can I check with you? Did you mean to send this? Is it authorised?
- Julian:** If something does go wrong, there's a mandatory reporting obligation. And that covers irregularities but also suspected irregularities. What's the process for that? And what would your advice be for practitioners thinking about, well, do I have a reporting obligation?

Sharon: So the first thing I probably remind listeners is there's a document we've generated with Lawcover. I would recommend everybody print it out. Now, I'm not a big fan of printed documents, but this is probably one document I would always encourage everyone to print out. And what it has is the key points of contact in the event of either a data breach or a financial breach.

Who is your bank's fraud team? What is their number? What is the number of the law society? How do you reach out to Lawcover? Because the minute you're attacked from a cyber incident, you don't have time to be going through your computer, and go, where's that email? Googling, where's that number? Have them printed on a wall and somewhere visible so that everyone knows in the event of ... we have to unplug all the devices, that's there - we can pick up the phone and ring that number. In the event of a breach, the first number to always call is the 1800 4BREACH. Lawcover can put you in touch with an external company who will do an assessment of your infrastructure and IT landscape.

And that's really important because what you want to know is: is there malware in your system or is the issue outside of your system? Then the next thing is if there's money involved to ring your bank's fraud team to put them on notice, put a stop in place. Then the third place would be to call us in the trust accounts department, you can notify us either online through a form, but a lot of times these serious ones, they just pick up the phone. Yeah, so in that document, it goes through if it's a data breach, there's a specific pathway. And if there's money lost, there's another layer of contacting the bank. And the reason you contact your fraud team at the bank is A, they can initiate an immediate trace. And the fraudsters love moving money fast. So when they take money out of your account, they don't just put it into one account, they put it into 30, 40 accounts. And then they layer it and they send it to 30, 40 other accounts. So in the space of seven minutes, they can move it to 170 different accounts. And sometimes when they move to the overseas jurisdictions, it can take days for the intermediary banks to come back with where the money has gone to. So that tracing, the sooner it's started, the better. So we've had the most success when people identify the problem and they have the "oh no" moment and they pick up the phone straight away, then we can help the banks to get straight away onto tracing.

Julian: It's a mortifying moment though, isn't it? And you can imagine that people just want to try and minimise the damage, probably don't feel good about contacting other people about what's gone wrong. What would you say to people who are feeling that?

Sharon: You know, it happens to everyone. So when it does and people ring up and I'm talking to them and you can hear that gut-wrenching pain, the angst, the frustration, the embarrassment, what would people think of me? What would my clients think of me? How was I so stupid? How did I fall for this? When I say to all of them is that it's human nature. They prey on lawyers. They know you've got a vast amount of accessible data, sensitive information, and a vast amount of money at your disposal in client trust accounts. So they target you. They go out of their way to develop scripts that are dedicated entirely to manipulating you. So it's not that you fell for it, they've gone out of their way to manipulate you into a situation of trust.

Sharon: So we have a service called So Well at the Law Society and I always refer people to that. It's a free counselling support service available 24-7, but also for law practice employees because oftentimes we talk to the principal who has the ultimate responsibility. But the staff themselves, the people who pick up the phone, who transfer the call, who clicked on the link in the email, they're mortified. So it's very important that they have someone to talk to, they've got a support and to know that they're not alone.

So once they call the bank and report it to the bank's fraud team, the next step then is to report the irregularity on the trust account to the Law Society. And they can do that in two ways. One, they can pick up the phone, the call is directly in the trust accounts department. Or 2, we have an online form. It's called a section 154 online form. It'll be available in the links for today.

Julian: There are formal deadlines for doing that, but you shouldn't be worrying about the deadlines. You've just got to do it straight away?

Sharon: Straight away, as soon as practical. But particularly where money is concerned, it's not about ticking boxes. It's really about trying to get that money back as quickly as possible.

Julian: If off the back of this conversation, Sharon, people want to get more resources about how to make sure that their trust accounting procedures are tip top and up to the minute, where should people look?

Sharon: So either on the Lawcover website or on the Law Society website, we've actually together developed four really useful, I think they're really useful, resources. And the first one is the Cyber Risk Management Checklist. So this is a practical checklist that covers all the key risk areas, including your payment processes, email fraud, and your data storage.

Now you might also be interested in Data and Cyber Security for Law Practices. This is a guidance on safeguarding your client data, how to respond to cyber incidents and generally meeting obligations when handling personal information.

The Cyber Fraud Prevention flyer, a one-page document that you hand to your clients when you're onboarding them to reduce the risk of cyber fraud. And this basically sets out that here are our trust account details. Here is the common phone number you can call us on if there's ever any queries, but also get their phone number. So what number should I call you on that I can verify anything? So you had that at the beginning.

And the final one that I always recommend everyone prints and puts up on their wall is the Cyber Incident Procedure and Emergency Contacts. And this is guidance to assist law practices in identifying, containing and responding to cyber incidents when they happen. So it's almost like the house is on fire. What do I do?

Julian: From everything you've told us, it is true - you have to trust no one.

Sharon Blake, it's been great speaking with you on Risk on Air. Thank you so much for joining us.

Sharon: Thank you so much and thank you to Lawcover for having me.

Episode 63
Trust No One

Outro

Thanks for listening to Risk on Air by Lawcover. And to stay up to date, join us for the next episode on current risks in legal practice.

Resources:

[Cyber risk management checklist](#)

[Data and cyber security for law practices](#)

[Cyber fraud prevention flyer](#)

[Cyber Incident Procedure and Emergency Contacts](#)

[Solicitor Wellbeing Service \(SoWell\) – 1800 592 296](#)

[Trust Account Irregularity Form](#)

[Additional Lawcover cyber resources](#)