

Procurement Block S1E8 Murray Raw

SUMMARY KEYWORDS

fraudsters, fraud, businesses, absolutely, procurement, murray, fraud prevention, organizations, opportunities, defenses, technology, check, people, individuals, target, superpower, bank, cricket, crime, pandemic

SPEAKERS

Murray Raw, April Harrison

April Harrison 00:03

Welcome to Procurement Block, a podcast all about digital transformation in procurement and supply chain and how blockchain risk management and change management all factor in. I'm your host April Harrison, Marketing Director for Trust Your Supplier. I'm a procurement novice eager to learn more from the people who are at the forefront of procurement innovation. On today's episode I am being schooled by Murray Raw. Murray joined Synectic Solutions in 2015, bringing with him a wealth of experience about the financial services industry and the insurance market. Murray's experience includes 10 years at one of the UK's leading credit reference agencies covering consumer and commercial credit, fraud, and it sails into some of the country's largest financial institutions. Murray is head of business development at fanatics and was responsible for leading the new business sales team. His focus is on consolidating the market leading position in the core sectors of finance and insurance. With his team Murray is also tasked with developing new markets in the existing territories and leading the expansion into new global markets. Murray has a Bachelor of Science degree in economics and computer studies. Outside of work, he is chairman of his beloved local cricket team and still plays. You can read more about Murray's background at procurementblock.com. Join us as Murray and I discussed the basics of financial crime. Learn how companies are managing the risk associated with financial crime, the role that technology plays, and what preventative measures should be taken by organizations and individuals. Murray is a cape-less superhero as he protects us all with insights to defend ourselves and our companies against the battle with fraudsters. Welcome to the podcast. Murray. I'm looking forward to our conversation today.

Murray Raw 02:00

Thanks very much, April. Yeah, me too. Absolutely.

April Harrison 02:03

Can you tell us a little bit more about yourself? You're a cricket player. Correct?

Murray Raw 02:09

I am just a cricket player. I'm almost too old. But I'm hanging on. But it's a game I absolutely love I've played since the age of 11. And yeah, I still turn out every Saturday for my club. But I'm I'm finding it harder and harder to keep going. I must admit.

April Harrison 02:26

Well, I actually attended in person my first cricket matches this year, I found it really fascinating. I'm still working out the scoring.

Murray Raw 02:34

I think it's one of those games where it's very easy to understand the basic principle, you know, I guess like baseball, you know, where you have a picture in it and a batter it pretty much the same in cricket. And the idea is to hit the ball as far as you can. So the basic principles, very easy to get your head round the rules, incredibly complicated. And yeah, for someone who's new to the game, I totally understand why you why you might struggle a little bit with the rules.

April Harrison 03:01

Yes, I'll need a primer on that before next season. So completely another completely non related topic. Let me start with a question I asked every guest, and it might be related to what we were just talking about. But if you had one superpower, what would that be?

Murray Raw 03:19

Okay, so I've been thinking about this. And I toyed with, I guess some of the ideas that I suspect you might get more often than not. And I thought about, you know, should it be that I'd like to sleep less? Because that means I could do more? Or should I slow myself, so I couldn't be more productive? And I thought about those sorts of answers. And I thought no, it has to come back to what we were talking about a minute ago. And if I had a, it's not even a superpower, but if I had an ability that that that I don't currently have it would be to be better at cricket, or better at rugby. And more than that, I would love to have represented England, either cricket or rugby, to sports I'm really passionate about and to my mind, the sort of pinnacle of either sport is to represent your country. And it's something that I was a million miles from achieving but something I would have absolutely loved to have done. So yeah, it's it's not a it's not a superpower as such, but it is something I would like to have been able to do much better.

April Harrison 04:22

That's totally relatable.

Murray Raw 04:25

Yeah, perhaps not the business related answer you might have wanted, but it's something like I said, that's important to me something I'm passionate about.

April Harrison 04:33

What I would like the ability to do is know a lot more about a lot of different things. So that's one of the reasons I have you on today. I am learning the basics around initiatives and technology within the broader area of procurement and supply chain. So I would love for you to kind of school me on the topic

of financial crime. And since I'm a novice, I want to start with the basics. What do we mean by financial crime?

Murray Raw 05:02

Financial crime is a bit of a catch all phrase that covers three main areas. Money laundering, terrorist financing, and most significantly, to to us as individuals and to businesses fraud. So it's a Yeah, a generic term covering those three key areas.

April Harrison 05:25

In those key areas, does financial crime pose a bigger threat today?

Murray Raw 05:30

Yes, yes, it does. But I suppose I should caveat that answer by saying that it has always been a massive issue. It's always been a challenge that businesses and individuals face long before the global pandemic, it was a major, it was a major challenge. You know, fraud has always been there organized fraudsters a very sophisticated, often one step ahead of those of us that are trying to prevent fraud, they're always looking for new emos. They're always looking for new ways to commit fraud. And they're always testing the fraud defenses of organizations, and the awareness of us all as individuals. So it's not something new. And it's always been a massive issue. I mean, certainly within the UK, the last stats I saw the cost of fraud to individuals in the last year that was reported was 4.7 billion pounds, the cost of fraud to businesses into the public sector was 5.9 billion pounds. And I'm sure that in the united states that the figures are exponentially larger. So it's not something new. But the pandemic has provided more opportunities for fraudsters, if you think about how we all have been forced to change the way we do things, both both in the workplace, and as individuals. You know, we've been locked down being forced to work from home, we've been forced to shop from home. So because of those changes, it's presented new opportunities to fraudsters. So if you think about people buying from shops can't transaction volumes have fallen off a cliff. But the the number of transactions carried out online has increased massively. So all of this change has provided fraudsters with new opportunities to exploit and I don't know about the United States, but certainly again, here in the United Kingdom Government has been implementing all sorts of schemes to help businesses and help individuals get through the pandemic loan schemes, Grant schemes, yeah, sort of income replacement schemes. Again, all of these provide massive opportunities for fraudsters. So the UK Government, for example, implemented something called the bank's bank loan scheme to support businesses through the pandemic. It's estimated that the potential losses from fraud from that loan scheme alone could be 26 billion pounds, remote banking frauds increased by 27%. Since the pandemic phishing scams have increased 53% viruses and malware targeting fraud have increased by 40%. I suppose the bottom line is fraudsters love change. They love disorder, they love new entrants to markets, because it just gives them more and more opportunities to exploit.

April Harrison 08:18

I'm wondering if technology plays a major role in the increase of this right, it's easier to access and to be able to hack or to commit fraud.

Murray Raw 08:29

Exactly that. So you know, if you think about the couple of examples I gave there, where, you know, we're all transacting more in an online environment, we're all applying for facilities on the internet, rather than going into the bank or, or, or whatever, you're all of those changes present opportunities to fraudsters. So technology whilst being amazing in facilitating a lot of what we do in today's life, and supporting the ability to work from home, for example, during the pandemic, when we haven't been able to go into offices. All of that's fantastic for us all for businesses and individuals. But again, it offers more and more opportunities to for fraudsters to commit fraud.

April Harrison 09:09

I've also noticed an increase online or in the news of things like ransomware things that I hadn't really heard of, previously, these hackers can take an entire country down to its knees by having controls over gas and oil or other necessities. Right?

Murray Raw 09:30

Absolutely. You know, and if you read about the sort of background to some of those, some of those hats, you know, it's it's state sponsored, you know, there are there are sort of malignant countries in the world that are targeting targeting as all the large organisation, government, etc. So yeah, it's technology is wonderful thing, but it also poses some enormous challenges to us.

April Harrison 09:53

Right, a double edged sword.

Murray Raw 09:55

Absolutely.

April Harrison 09:56

Are procurement organizations placing enough importance on finance crime? Seems like it would be hard to ignore that in this day and age.

Murray Raw 10:03

I think you're absolutely right. So, you know, we're seeing a transformation in the way that businesses procure goods and services. The automation of that process is fantastic. It allows you to streamline processes, to widen your reach to speed up the procurement process, but haven't come back. Coming back to the point we were speaking about a moment ago fraudsters love change. So if you automate the procurement process, but do so without having the appropriate fraud defenses in place, there's a potential that all you're doing is speeding up automating, and making more easy the ability of fraudulent organizations to transact with you. So again, that that double edged sword that you mentioned a minute ago, but you know, the changes that we're seeing in the procurement process and procurement systems and the automation of it, fantastic, absolutely brilliant. But there is that double edged sword because it provides opportunity to fraudsters.

April Harrison 11:03

So it almost seems like yeah, that automation, sometimes it doesn't allow for oversight as to who is actually accessing the information.

Murray Raw 11:12

Well, I mean, there are certainly lots of ways that organizations can have that oversight. But it needs to be you know, you need to take an holistic approach to the deployment of any new system of any business process automation, because you know, the benefits to the business, the streamlining the cutting of cost, as I said earlier, that broaden your reach. So you can you can reach more and better organizations to procure goods and services from all of that's fantastic. But you need to know who you're transacting with. And you need to know that they are not fraudulent, that they're not going to try and try and perpetrate fraud on the organization. So it's Yeah, it's not that the systems aren't there, it's just that when you are looking at business process change, you need to consider all of the implications of it, and make sure that you have the appropriate defenses in place.

April Harrison 12:00

So how are companies managing the risk associated with financial crime?

Murray Raw 12:05

I think it very much depends on which sector we're speaking about. I think historically, financial institutions and insurers have well established processes, and for the most part, very sound and secure fraud prevention systems. And that's driven by risk, you know, lenders, clearly a targets, and in the insurance world, insurers of target, perhaps at point of sale, but most often at point of claim, because there are huge opportunities for fraudsters, but it's I think, sort of a fair comment to say that fraudsters target the low hanging fruit. So they'll go where the opportunity is, which is obviously Firstly, where they can make make the most money. But secondly, where they can do it most easily. So what you'll find is that as certain sectors, certain organizations build their defenses appropriately, or we as consumers change our behavior, so we become less targeted, so the fraudsters will go and find new ways of, of perpetrating fraud. So if banks and insurers, for example, put up their defenses, the fraudsters very quickly realize this, they're very quickly No, because they're always testing systems. They're always testing processes, they'll go somewhere else, they'll look for new and different opportunities. And, you know, I touched on this at the beginning, we try and be proactive, we try and anticipate where the challenges are, and build defenses accordingly. But equally, sometimes you have to be reactive. You know, the fraudsters are clever, they will just target and they'll target new entrants to markets, for example, you know, if a new bank comes along, or a new lender, and they don't have the appropriate challenge defenses in place, fraudsters will target them they'll nail down those through the press that there's going to be a new product or a new, a new credit card or a new loan from a from a bank. And they will deliberately target those organizations and seek to find weaknesses if there are any. And I'm sure it's the same within the procurement world. Again, as you automate that process. If businesses don't have the right defenses in place, they run the risk of being targets.

April Harrison 14:10

From a personal level, I think about all the porch pirates, one of the things that I see that people put in place are those doorbell cameras, to be able to identify people who come and take their packages, that kind of thing. What kind of role does technology play and managing financial cameras?

Murray Raw 14:27

It's absolutely paramount in fraud prevention. So think back to our conversation a minute ago about the automation of procurement. You can't drive innovation in any area of the business and implement them if you know, sort of automate business processes speed up what you do, if you then implement, for example, manual processes to check. So coming back to that procurement example, you automate that whole process, you widen your reach you make it easier for people to transact with you. And then implement slow clunky man Do checks on all those organizations, you have to be able to use technology to align your fraud defenses with your business process automation. So think about it in terms that perhaps you and I would understand APR. So if you, if you apply for a loan, any of us these days, we want instant gratification, don't we want to be able to apply for a loan and get an instant decision. And we want automatic release of funds. Or if we walk into a store to buy a new television, and we apply for finance on that television, you want to be accepted immediately. And you want to be able to walk out with that new television under your arm. If it's not too big. So you know. So, again, we, as consumers want that automatic decision, that automatic release of funds, we want to know immediately that we can have what we want for us as providers of fraud prevention solutions, we need to align with that. So we need to be able to in absolute real time, provide checks, send them back to the lender to say yes, you know, APR is not a fraudster, yes, you can you can safely progress with that application for a loan, you know, knowing that you've conducted robust checks, and she's absolutely fine. Release the funds, let her have that television. So technology is absolutely fundamental. it's incumbent on organizations to implement strong defenses, but ones that don't impinge in any way on the customer journey. So you're absolutely right, technology is a vital part of the whole process.

April Harrison 16:37

I never thought about that need for instant gratification and how that would play into this process. So...

Murray Raw 16:43

But it's it's the way of the world, isn't it? Yeah, we as consumers behave like that. But it's the same in business, you know, again, decisions are expected very, very quickly. It's interesting, actually, with some of our clients where, you know, within clients, we deal with the fraud prevention teams, but they've got the marketing and the sales teams demanding this seamless customer journey, this seamless onboarding journey. And there's sometimes conflict between the two, because fraud, want to put barriers in place and do your checks that perhaps take a while to you know, to before they then allow the customer to get whatever good or service that they're seeking. So we as service providers have to make sure that our services do work in real time, and that we can provide the robust checks. But without getting in the in the customer journey in the way of the customer journey at all,

April Harrison 17:32

What other preventative measures should be taken by organizations.

Murray Raw 17:36

So coming back to the above, there are lots of technology based solutions that are available. And those technology based solutions have the ability to call out to numerous predictive data sets. So yeah, that allows businesses to rapidly check to ensure that they know, you know exactly who they're speaking to, that those people are, you know, businesses are, who they say they are. And not only that, but you know, they haven't had any sort of history or record of committing fraud elsewhere. So there's, you

know, there are lots of solutions out there. And the more interesting ones for me that sort of newer systems around device identity, email identity, telephone identity. So there's all sorts of really exciting developments in those sorts of areas. So you know, when, again, when an organization or an individual contacts you via the internet channel, you can understand everything about the device that they're contacting you from? Is it where is it, you know, if it's a company, saying that they're in Atlanta, in Georgia, but actually the IP address happens to be in in West Africa or in the Far East or in Russia? and tells you something about that that business that you're dealing with or that individual? Or if the email address that they're using to contact you from was created yesterday? And isn't linked to any bank accounts or isn't linked to any social media accounts? Does that tell you something about that application about that business about that person? You know, if the email address was created 10 years ago, and is associated with a number of financial instruments, then does a degree of reassurance about that. So, you know, there's all sorts of very interesting and different data sets that can be deployed as part of a fraud prevention solution.

April Harrison 19:25

Yeah, that's a larger scale to what I've been trained to do on a personal level, which is, you know, when I receive an email, you know, I double check like the URL, you know, to see if it's misspelled or, you know, I don't ever click on the link in there, I go directly to either my, my bank's website to log in, rather than clicking through the email.

Murray Raw 19:46

Yeah. And you know, those are really sensible things that we all should be doing. You know, you mentioned earlier that you've seen a huge increase in in online scams. Yep. We know I'm sure all of us I'm sure everybody listening has been targeted by fraudsters authorized push payment fraud, social engineering, phishing scams. I was talking to someone earlier actually, who said that the word scam shouldn't be used, you know, scam is a it's it's sort of belittles the seriousness of this, you know, the cost of fraud is massive, as we spoke about earlier, the social cost, you know, sadly, a lot of fraudsters will target the old elderly and the vulnerable. Because, again, coming back to my comment about the low hanging fruit, you know, fraudsters, we know that they will target the easiest people to defraud. So there's this been huge increase, we've all received these emails saying, you know, your, your bank account has been compromised, click here, or phone this number. You know, it's, it's, it's endemic. So

April Harrison 20:55

it takes me a little bit longer when I'm looking at something to determine if it's, you know, fraudulent or not.

Murray Raw 21:03

Absolutely, I mean, we had an incident recently here at work where someone in our finance department received an email purporting to be from our chairman and owner, saying, I really need an urgent sort of job, I've got an urgent job for you, I need you to transfer some money from this account to this one, unfortunately, I'm on holiday, unable to do it. And our chairman was on holiday. And so it was either very lucky, lucky guests from the fraudster, or somehow, they knew that the chairman was on holiday, and they knew the contact details of someone in our finance department. And they targeted them. The person, the finance department, obviously didn't act on it. But you know, it's incumbent upon

us all to be aware of how these frauds are perpetrated. And like you said, Just take your time, just check. Look at the URL, you know, just be aware that all these things are out there and just pause before you act.

April Harrison 21:59

Very, very good advice. Speaking of advice, to have any that you would be willing to share with me and our listeners.

Murray Raw 22:07

Do you know what I think I think you've asked the questioner already. By saying check the URLs, you know, look for, for misspellings look for anomalies. And you're absolutely right, that the fraudsters are becoming more sophisticated, and the emails that they send out, look more and more realistic. But yeah, little things. So if there's a link to click, don't click on it, just hover over it. And if you hover over it, the address that it does take you to will come up. And you know it, is that link to the bank that has purported to send to have sent the email in the first place? Or does it look unusual? You know, is it a series of letters and numbers? So it's that type of thing. Just Just be aware, and pause. And if you've got any concerns, wring the bank, check with them? So I just, I think it's more about awareness than anything else, you know, if we're all aware that we are the targets, were less likely to be fooled.

April Harrison 23:04

Yes, I will have to say I enjoy those YouTube videos where people try to, to scam the scammers. So they might put a fake box on the porch. And when the porch pirate comes and tries to take it, it explodes, sprays, paint all over them or something. It can be entertaining sometimes. But it's sad that we live in a world where we have to protect ourselves like that.

Murray Raw 23:28

Oh, absolutely. But you know, the fact that those sorts of programs exist on the television or on YouTube or whatever, I guess it's good in a way because again, it increases our awareness and makes us think about what's out there.

April Harrison 23:40

So very, what projects do you have on the horizon?

Murray Raw 23:43

Within the UK, we have lots of consortium databases that we use for fraud prevention. So you know, lots of banks and lenders and insurers sharing and pooling data. So data protection laws, allow it and conventions of across businesses means that it is accepted that data sharing for the prevention of fraud is an acceptable practice. So we're very, very lucky in that respect that we have access to a wealth of data that helps us to prevent fraud. That's not necessarily true in all global locations. So we've been thinking about, well, how can we how can we address that? How can we help sort of fill that gap? So we've been working very hard recently on building machine learning sort of base scores using advanced modeling techniques and powerful algorithms fed by all of the data that we have access to, we've got access to absolutely vast amounts of fraud related data. So we've been building global scores in finance and insurance and you're different markets that that hopefully can can be deployed in,

in areas where, where this idea of consortium data perhaps doesn't exist. So we've been getting some quite interesting results from that recently. So I suppose that's an interesting for me a very interesting development into a new area that helps, again helps us spread our, you know, our sort of what we're passionate about which is, which is preventing fraud.

April Harrison 25:15

Absolutely. That's brilliant. Murray, thank you so much for schooling me on financial crime and best of luck to your cricket team.

Murray Raw 25:28

And we'll need it. Thank you. And, you know, thanks for giving me the opportunity to speak to you it's been great. And as I said a moment ago, I'm passionate about sort of fighting fraud, so any opportunity to, to discuss it with people to share views and help in that that sort of global battle against the fraudster. And you know, I'm up for it any opportunity. You're very welcome. So for you or anybody else has any questions for me I'll happily happily failed them.

April Harrison 25:57

You know, you don't need a superpower. You are a superhero. I think you need a cape, like protecting us from all this crime.

Murray Raw 26:05

I need a new knee so I can continue playing cricket. That's what I need.

April Harrison 26:11

Well, it's been a pleasure. Thank you so much, and take care.

Murray Raw 26:16

Absolutely. Thanks so much. for your time. It's been it's been great talking to you.

April Harrison 26:21

That's it for this episode of procurement blog. I'd like to thank my guest Murray Raw for joining me on the show. Procurement Block is produced by Trust Your Supplier, you can reach us at procurementblog.com. Show notes are available on our website, and you can leave your questions and comments via the listener comment form. Thank you for learning with me today. I'll leave you with wise words from Benjamin Franklin, "An investment in knowledge pays the best interest."