[Introduction]
With the rapid behavior changing disruption of recent years, and the ongoing stream of corporate governance failures. ACCA has been digging deep into how interconnected risks such as climate change and geopolitical issues are influencing the way we approach risk management. This podcast series will look at what risk culture means and to what extent risk and accountancy professionals understand its impact on performance.

[Voiceover]
Fraud is rampant and pervasive all over the world and our profession is under increasing pressure from regulators and other stakeholders and society at large to get a better handle on it, especially as generative AI and all of the rapid transformations we are experiencing, only exacerbate such risks. So who better to talk about the power of whistleblowing and how our profession tackles this than Emma Perry, a conduct culture and risk advisor and core member of ACCA special interest group on risk culture, and Pav Gill the Wirecard whistleblower and CEO and founder of the Confide platform. Hello, both. It's such a pleasure having you with us for this episode. Let's start with you, Pav. I'm sure our listeners will be eager to hear about your experience. So could you share with us what the lessons in hindsight are and what led you to set up confide?

[Pav Gill]
I think the biggest lessons from the Wirecard scandal is where did things go wrong, right? Like internally versus externally, it seemed to be such a systemic and systematic collapse, you know, of control functions internally, as well as external bodies that you would think would have played a part in preventing this scandal from happening. You know, internally, we're looking at internal audit teams, we're looking at legal and compliance, corporate governance structures, how effective were they? Even though they might have been in place on paper? Were they actually effective? Where were the weaknesses? Can we even blame them for what happened? And then if we look externally, like how did this thing go unchecked? How did this beast form over 20 years, that despite so many efforts to raise concerns with the company, no one did a thing. We had a failure from the external audit side, we had a failure from regulators side the BaFin, for example, in Germany, law enforcement in multiple countries, did not act despite whistleblower reports. So I think that's just shocking. It's funny that you asked what lessons were learned? I have no idea. But those were the lessons we can learn in terms of what do we do? And where can we put the spotlight on in terms of my lessons as an individual as a professional as well, I think we should always continue to look at what's concerning, and never shy away from raising those concerns. Because what we also need to remember is that if we don't raise those concerns, we can be sucked into the whole process of being part of that problem, right? Being part of the potential wrongdoings that are happening within the company. So I think it's very important to do your job raise those concerns, as the most basic fundamental start. That has naturally led me to found Confide because I think it was very unique set of events, right? That all converge into one point. Firstly, having seen these things from a control functions head angle, as head of legal for multiple companies, and of compliance as well in those roles overlapping somewhat, and then also being a whistleblower in the process, very unique combination. So I thought why not just put everything into a product, a product that would benefit companies as a risk management, early detection tool prevent another Wirecard from happening, hopefully, you will benefit employees and staff vendors, everyone, you know, it gives them that safe space. Often people don't know who to confide in, right? Like, oh, you might be over confiding in people. Or you might even be prevented from confiding in the first place like you've got legal privilege and other confidentiality restrictions imposed on you. So that's how I decided let's just create this company and create that space, benefits corporations, employees and lawmakers, because you're helping them achieve their regulatory objectives.

[Voiceover]
You did explain what Confide is, but a little bit more how it works with the clients or what stage you are now in the development?

[Pav Gill]
So the idea at least my mission of the company, is that I want to see less of that caricature type whistleblowers right? Disgruntled, angry, isolated person that realizes there's nothing within the company that works or is trusted. And the only solution as a result of this is to go externally. And externally, there's two components to it. One is The regulatory law enforcement side. And then there is the immediate side. In many countries, especially developing countries, they also might be concerns where regulators and law enforcement are in play, can they be trusted? Will they weaponize this info and expose me? Or even worse, monetize this information and expose me? So what does that leave whistleblowers with? It's just the media, right? But is that really the outcome that companies want? I don't think so I think if we've got a good corporate governance tool in place like a whistleblowing tool, we can minimize or at least in a more responsible way, deal with these things. Your audit log is there, it's up to you how you want to deal with whistleblowing reports as a result of it is now traceable. And you also can go to your IT team, say, I want to know who sent this email to company name and whistleblowing.com, I want to track this person down. It's all offline, it's in a secure environment, you can liaise with the whistleblower in that environment. And from a whistleblower's point of view, it's giving you the opportunity to follow internal protocol, not have to go outside, and also gives you that visibility and power, I would say, to see how the company is going to deal with this concern. And from an educational standpoint, you're learning each step of the way. What's dangerous is that many platforms out there, while are many, many processes out there might say this is a whistleblowing process or this is a whistleblowing solution. But there's no education involved. So someone using the platform for #MeToo case or speaker case, might be under the false impression that they are equally protected under the law as a whistleblower, versus someone that's actually going to use that tool to report like a breach of a new regulation. So I think these are very important concepts, which whatever tools you might have needs to address. And that's what we're trying to do with Confide.

[Voiceover]
Thanks so much for sharing your experience with us Pav indeed, there is a lot for us as accountancy professionals to reflect on how we can help foster cultures that encourage employees to speak up and feel safe? So Emma, over to you, how would you describe the breeding ground for fraud today? And what would your message be to accountancy professionals in terms of detecting and combating these acts?

[Emma Parry]
Thank you, great to be here today. So the regulatory expectations, actually their obligations around doing, for example, risk assessments that include the risk of fraud. Fraud is one of the broadest typologies we're looking at both internal and external fraud, criminal cases. And so the risk assessment needs to look at what could arise in your business based on what it is that you're doing the nature of the business supply chain, types of clients, jurisdictions, products and services. So that's the starting point. And that's what the regulator's will look for, in terms of behaviors and what we're seeing in the regulatory space. I think what has become quite important, and this really came out through the pandemic is the way in which regulators are trying to tackle fraud in a multifaceted way. And I'm talking primarily from a financial services regulatory standpoint now. Obviously, they've set out already in the UK, for example, clear guidelines on what constitutes a fraudulent offense, we've got various acts, and now we've got the online safety bill as well. But they're also a tackling fraud in other ways. So raising awareness through their website, so in the UK, we've got the FCA Scam Smart, which talks about and helps to educate the public around what scams can look like fraudulent activity, their speeches, warnings, press releases. But one of the most interesting cases that I came across again, this is during the pandemic is, for example, ASIC in Australia, actually disrupted a campaign directly on a social media platform. So it actually joined and disrupted a chat that was being used to promote market manipulation scheme, a type of fraud. And so, you know, we are seeing more dare I say, agile ways of the regulators trying to tackle these things. Additionally, there's collaboration activities. We're looking at IOSCO as a prime example of that in the security space. We've got more focused on things like public and private

partnerships. So SPF police force, announced in October of this year that they're joining forces with Meta to tackle WhatsApp scams, which I think is a really interesting development in that space. We've got more focus on cross border considerations as well. In the UK. We've got the online safety bill which has an extraterritorial effect. So it encompasses platforms that have links with the UK. So this means that any platform with a significant number of users In the UK can be or falls within the provisions of this Act, which I think is a really interesting space, it helps in some ways to address regulatory asymmetry. So trying to get greater, I guess, global consistency around enforcement action. And speaking of enforcement actions, one of the biggest ways to try and deter this type of activity is obviously through enforcement. And so we've got here again, the UK, a communications regulator, Ofcom can impose fines of up to 18 million pounds, or 10% of the providers worldwide annual revenue, whichever is higher, you know, as ways to enforce and penalize fraudulent activity. So there are lots of things going on in this space. I think one of the most key things from my perspective, is the educational aspect around the retail investors, particularly because if we look at some of the investment scams and fraudulent activity, they're the targets, and they need to be continually reminded around the dangers that are lurking.

[Voiceover]
Do you have anything to add on that Pav?

[Pav Gill]
I think it's only so much we can hide behind speed of tech and development from a regulatory or legislative standpoint, right? If criminals are evolving, then all the more the other side needs to evolve as well, we can't always be playing catch up. If you look at that in the hacking space, for example, you have companies that actually pay 'white hat' hackers to get ahead of that curve. They don't wait for something to happen, and then say, OK, now that has happened, let us find a solution to it. So I think given plus the resources that government agencies will have backing them, that is, at some point, it's going to become a weak excuse to always say, oh, we can't keep up with you can't keep up with it. Because you have the resources, you have the brain power, and the ability to do so. So that's just my rather strong point of view. It has evolved over the years, of course, given what I've been through as well, you know, and that's also what Confide doing, right. And one of the things that just this weekend was thinking about is that whistleblowing is a human problem. It's an emotional problem, primarily, if you break it down. It's an emotional problem from the person reporting because there's all these things like trust involved, and, you know, wanting to raise these concerns not being able to do so and so on. And then from the company standpoint, there's always that emotional problem about, oh, we need to make this go away. What do I do to make myself appear more useful to you know, potentially the powerful ones who are paying my salary? So, you know, we have real standpoints and all the psychological aspects involved. So at some point, maybe the solution would be to take the human aspect away from it from a subjective standpoint, right? Should we create tools that can strip reporting of its emotional aspect, and also just then help companies help people focus on the objective side of it, you know, something that will guide and influence you towards the call and the substance of the issue. So I think AI has a very strong potential in that space. And that's something we're definitely looking to explore, just to be ahead of the curve and try to just think more out of the box as to how we can solve these human issues.

[Voiceover]
What misconduct issues concern you most in financial services? And where are the blind spots in this industry that you see now?

[Emma Parry]
So, in terms of misconduct, and where I see some of the blind spots, just to build on Pav's point is around what we're seeing now in terms of what I'd call turbo charging of fraud, where fraudsters are now exploiting AI and deep fakes to run scams. And we've also not just got single perpetrators now, but organized syndicates, and also we've got crime as a service. So we're fraudsters, are leveraging capabilities across the criminal network to fill the gaps in their fraud schemes. So fraudsters

are exploiting gaps and opportunities faster than we can keep up in terms of regulation, detection and prosecution. So I think there's a few blind spots that we need to start addressing as an industry. And again, I'm talking from financial services particularly, we've got siloed reg tech solutions. So we've got things like financial crime siloed solutions, and then Ecomms and trade surveillance solutions. What we need to do is to have an opportunity to bring those insights together, we reduce the siloed data that prevents us from understanding the network of fraudulent activity that sits across for example, payment accounts, who the beneficial owners are capital markets transactions. I suspect there's a lot of criminal activity that's actually hiding in plain sight in our data that is sitting in the silos. And I think the other thing that is hampering our speed as an industry is capability asymmetry. And what I mean by that is where we've got firms that may have limited resources, and may be relying on spreadsheets, while regulators and other say the tier one banks are already exploring or using AI powered, or in this case, market surveillance solutions. So whilst we have asymmetry in the industry, fraudsters will continue to exploit the gaps. And I think this is also where collaboration is key public private partnerships, which I've mentioned, are ways in which we can keep up with the fraudulent activity.

[Voiceover]
Thanks Emma, that was brilliant. OK, both of you just end on what your message would be to ACCA members, so accounting professionals, and then Pav, let's start with you, thank you so much.

[Pav Gill]
I think the message to ACCA professionals is really to just believe in what your job requires and do it. I think you need to be comfortable with the fact that you have done your job well, you can sleep well at night, as a result of it, you're not going to be flagged for any kind of negligence or oversight issues down the line. I think that's just the most important message that I would have, like, just stand by why you became an accountant, why you're doing what you're doing every day, and just raise those pride levels in that space.

[Voiceover]
OK Emma, now to you.

[Emma Parry]
Yeah, my final message to the accounting professionals, actually there are three things very quickly. So the importance of cognitive diversity. So we want to be creating an inclusive culture that welcomes and embraces differing views and experiences and input. And depending on the role that you're playing within your organization, ensuring that you're bringing those voices to the table. So if you're in leadership role, making sure that you are actively pursuing diversity, and if you are at the table, making sure you're active and engaged. But the final point and it just resonates with Pav's points is the importance of fostering a culture where people feel confident, encouraged to speak up, and we all play an active and important role in making sure that that happens.

[Voiceover]
Trusted information is crucial for building resilience and positive risk taking. And as we continue to advocate through this podcast series, accountancy professionals can serve as risk culture, 'super networkers' supporting teams and making informed decisions and sharing knowledge within and outside the firm. By telling the stories, our profession can raise risk awareness, promote new insights, and effectively influence the performance of the organization.

ACCA’s professional Insights Team seek answers to the big issues affecting finance professionals. Find our latest research at ACCA global.com forward slash professional insights.