Inside FCA Podcast: Interview with Emad Aladhal on fighting fraud and financial crime

OI: Hello and welcome to the Inside FCA podcast. I'm Ozge Ibrahim, and today I'll be speaking with Emad Aladhal, who is the director of a team of specialists working across financial crime, financial resilience, insolvency, safeguarding and operational and technological resilience at the FCA. He also co-leads the FCA's commitment on reducing and preventing financial crime. I'll be asking him about fighting fraud in particular, and what the FCA expects to see from firms.

Hello Emad, welcome to the podcast.

EA: Hello. Hello, Ozge.

OI: What's the FCA's financial crime strategy?

EA: The FCA's 3-year strategy started last year, and the strategy is focused on delivering two things that are very big things. One is on reducing money laundering and the other is reducing the growth of fraud. Specifically on fraud, we've all heard the stat before - 40% of crime in the UK is fraud. That's staggering. It should make us all pause and think about that.

OI: So what tools does the FCA have to reduce and prevent fraud?

EA: I want to say at the outset it's the whole FCA approach, and by that I mean I co-lead this area with my colleague Mark Francis in enforcement. So, you have both supervisory policy and enforcement right there, but you also have authorisation. You have our work on comms, in particular ScamSmart, and we use our broadest toolkit and I'm happy to go into detail.

OI: So yeah, you use the broad toolkit you've spoken about. Are there any other examples other than some of the campaign's work that you've just referenced there?

EA: Yes, and ScamSmart, so I think if we take a step back and we think how the FCA broadly looks at fraud, we look at regulated firms and making sure that they're doing their part. We look at our perimeter to make sure that fraudsters are not operating within it. And then finally we look at consumers and making sure that they are in the best place possible to identify fraud and not to fall victim to it. In that last piece, we have ScamSmart, as one of our leading pieces of work. ScamSmart is really focusing on trying to get consumers better sighted on the potential for fraud, become less susceptible to it. Our research indicates that consumers are now better informed through that work.

ScamSmart I think started in October 2014. Over 2 million people have visited the website. Over 270,000 people are using it and have used it to look at the warning lists. And we know through our engagement on the consumer hub, about 57% of those who called our consumer hub are doing so before potentially falling victim to a fraud. So, it's having that preventative control that we want.

OI: And are you using any of the FCA's data or different technology to fight fraud?

EA: Absolutely. So we have fraudsters who are skirting our perimeter. And what we're doing here in that space is using machine learning, web scraping, to identify where fraudsters are potentially advertising on websites scams or frauds. So, in any given day, we are web scraping about 100,000 websites. Through that work in the last year alone, we've issued hundreds of website take downs or asked them - the provider - to take those websites down and issued almost 2000 warnings off of that work. We've also engaged social media platform firms like Google, so that they establish policies to prevent fraudsters from using their platforms to advertise scams. We've had a remarkable change in that space. So those platforms and those search engines that have introduced policies have led, in some instances, to almost 100% measurable reduction in paid for scams.

OI: And can you tell me a bit about the trends you're seeing on fraud and scams that consumers and businesses should be alert to?

EA: Yeah, so fraud is unfortunately not a static activity. We're actually against organised criminals out there who evolve and who, as much as we are using the best tools and evolving our toolkit, they are evolving theirs. I'm sure some of those listeners today are aware of some of these examples, but we are aware that fraudsters are using artificial intelligence tools.

You know, one particular example that's almost scary is, is that that individual that a parent picks up the phone call thinks it’s their son, but it's not their son. It's their voice being spoofed using that technology and made to believe that, that they're in trouble in need of money. And we all saw recently the article or even looked at the video itself of Martin Lewis, not Martin Lewis, but artificial intelligence made to look like Martin Lewis. Those are scary, and those are trends.

OI: And who are your partners in the work to tackle these sorts of scams? Assuming that obviously this isn't something that the FCA is going to do on their own.

EA: Thankfully, we're not alone, both the private sector and the public sector need to do their part. And so in addition to the FCA, you have the Government, the Treasury, the Home Office. You also have the National Economic Crime Centre and other law enforcement parties involved. But also the private sector needs to be engaged, and they are engaged. So we're talking about the regulated firms, we're talking about telecoms, we're talking about social media firms. All of us need to play our part to come together. And we are doing that. And thankfully, under a recently agreed umbrella; the National Economic Crime Plan and the National Fraud Strategy agreed earlier this year. That gives both the private and the public sector some key deliverables that we need to work together on.

OI: We know that authorised push payment or APP fraud is a growing issue. Can you explain what this is exactly and the work that goes into tackling this problem?

EA: It's a growing issue, you're right to say that. Last year I think the numbers were astronomical. They were in the hundreds of millions. Something like £480 million of losses were due to authorised push payment fraud or facilitated fraud. Authorised push payment is how we make payments. Occasionally we log into our apps, and we instruct for a payment to be made to someone we're sending money to. But fraudsters intercept that. They fool us - individuals, us consumers - into making payments because we're thinking we're paying a relative or we're thinking we're paying for a product or we're helping a charity or otherwise. But actually some of this is fraud. And our work is really involved about trying to make sure that the regulated firms, those who provide payment services, are doing their part to put us on notice that this could be a fraudulent activity, and where they are cited that it is fraudulent, i.e. the receiver is fraudulent, they were there to stop us. So, we are working with the Payment Services Regulator, our sister authority, to help us achieve that response, both in terms of policy change as well as a supervisory change. And I can go into more detail if you want.

OI: Yes, please do.

EA: So in the policy space, the PSR is making changes such that there is mandatory reimbursement, subject to some limited circumstances, for those who fall victim to APP facilitated fraud are provided that cash reimbursement to make them good. That will have a dramatic change in incentivisation of regulated firms to look at how they are identifying those kinds of payments that are potentially fraudulent, pausing on them and seeking to make sure that they are right before they go through. We ourselves are also undertaking supervisory assessment of payment services firms and banks who provide payments services. We're looking at - it's a multi firm review - we've looked at a number of firms, that review is just in its final stages now. We're looking at how those firms have adapted, both in terms of how they identify payments that could be fraudulent, and also what they are doing to make sure the consumer is aware, and that the consumer is taking steps to prevent falling foul to fraud. As I said that work is about to complete.

OI: And what else do you need or want to do in this space, in terms of what you've talked about, there's a multi firm review coming out. Do you envisage anything different that you'll be doing or is that something you can't say at the moment?

EA: We're going back to those individual firms at the moment, so I can't really spoil too much because I think we need to speak to them, and then we are going to publish our final results for all firms to see and how industry looks at it. I would say a few things though. Firms need to look at what they are doing now in response to the consultation, I mentioned about PSR. And not only about how they are going to provide the disclosures, but how they are improving their systems. Your question earlier on this podcast about trends, and we mentioned artificial intelligence. We are seeing firms respond to that. We are seeing firms using sophisticated technology, looking at behaviour in customers' use of their apps to see whether it's unusual, and if so, whether that's a tell-tale of potentially a consumer being coached by a fraudster. So, as much as the fraudster is using technology, we hope firms are utilising that technology and improving their controls.

OI: There's been a recent increase in people being hired to act as money mules, driven in part by the rise in the cost of living. Can you explain what this means and what is being done to address it?

EA: Money mules is unfortunately where individuals are either unwittingly or actually knowingly being used or their accounts, their bank accounts are being used, to receive fraudulent payments from multiple parties before then it's passed on to a fraudster's account and then cashed out. The fraudster is trying to use them to receive multiple payments and hide their tracks along the way. We have some work on money mules. We are looking at payment services firms, looking at their controls to identify how they spot their customers being used as money mules and trying to make sure that those firms have active systems to identify that and respond to it, and either shut the accounts or get involved with the customers and make sure that they're doing the right thing. Last year, I talked about ScamSmart, but last year we did also a programme of work, and we were reaching out to consumers making sure they understand the consequences of being a money mule. Making sure that they understand that this is a criminal activity, and that they do not fall foul unwittingly to this kind of business.

OI: And you've talked about your expectations of firms there. What else do you expect from firms broadly in preventing fraud?

EA: Share intelligence. So, firms on the front line, we should be under no illusion to commit fraud and to get away with it and to cash out, the fraudsters will need to be active in the financial services industry, they will be utilising firms. So, firms need to help their customers not fall foul. But they also need to make sure that their platforms are not used by fraudsters. And then they, their lessons, their approaches, the intelligence they have, they need to make sure that they are doing, in addition to the legal minimum in terms of sharing intelligence, they are actively engaged, sharing intelligence with law enforcement and through their associations, sharing typologies so that we all can learn from this and respond to it as a collective.

OI: Are there any examples of good and poor practice that you can share?

EA: In terms of poor practices, both in terms of the investment fraud and APP fraud steer, we see good practices where before one makes a payment, they are given a warning, asked to verify certain information, asked about whether they have been coached into responding in a particular way. Those reminders, they may be simple, but actually are really powerful in changing and making a consumer pause. We see good practices also in terms of how firms react to customers who are subject to fraudsters. Not only are they responding to that particular individual case in the fraud, and helping address their concerns, but they are using it as an opportunity to learn about a typology, about a method of fraud, and then playing that approach back into how they fix their systems or improve their systems associated with that fraud. These are examples of good practices.

OI: And finally, what are the implications for firms that don't meet your expectations?

EA: As this podcast illustrates, financial crime is incredibly important for the FCA. It goes to the heart of protecting consumers and confidence in the market. We therefore expect all regulated firms to play their part. To make sure they are protecting their consumers and also identifying fraudsters that could be utilising their platforms. And we will use our supervisory toolkit and, if necessary, our enforcement toolkit, to achieve that aim.

OI: Thank you for your time today, Emad. You can find more information about the FCA strategy, including the work on financial crime and fraud on the FCA website. For now, I'm Ozge Ibrahim, I hope you can join us again soon on the Inside FCA podcast.

ENDS