NATALIE GRAHAM

mosaic moment

PODCAST_05

FIGHTING FRAUD LOSS

TOM FILBY

INTRO

0:01 **Got a moment? Fast changing risks affect people, businesses, and economies in today's turbulent world. Perils like cybersecurity, political violence, or threats to financial institutions. Listen in as Mosaic Insurance specialists quiz fellow experts on trending industry topics. Welcome to this Mosaic Moment.**

0:22 Hi, everyone. I'm Natalie Graham, Global Head of Claims for Mosaic Insurance, and I'm joined today by Tom Filby—a friend and former colleague. Tom is a partner in the insurance and disputes team at Mills & Reeve in London and he focuses on financial lines risks. Tom and I have been speaking recently about the perception within the insurance market that once funds have been paid away to a fraudster and have been indemnified by insurers, that that's it, that those monies are gone. The fact that the insurance industry perhaps isn't doing as much as they could to pursue recoveries. So, I've invited him here today to talk about his experience. So, welcome, Tom. Perhaps you can just start briefly by discussing kind of the 'how' of recovering monies that insureds have paid to fraudsters, for instance, after social engineering.

1:12 Absolutely. And thank you very much, Natalie. There's often the perception that once funds have been paid away to fraudsters, they're gone forever, and nothing much is then done—the towel is effectively thrown in. But having affected a significant number of recoveries over the years, I'm a little bit more optimistic than that, let's say. There's an array of legal mechanisms available for responding effectively to frauds. There's obviously the nuclear options, like freezing injunctions and proprietary injunctions. But more often, successful recoveries come from a much more subtle and incremental approach. One which I would say obtains sufficient information to then determine whether a credible and valuable opportunity for a recovery exists, and if it does what it looks like: in that regard, I'm a big proponent of what we call a 'Norwich Pharmacal' or 'Bankers Trust Order,' which is effectively a court-sanctioned mechanism that compels banks, to which stolen funds have been sent, to disclose full details of the identity of the recipient account holder, and provides a copy of their statements of account with all recent transactions. And this level of detail and insight into the recipient's account can provide a hugely informative picture as to the identity and nature of the wrongdoer, and the status of the funds and whether they might have been blocked, or onto where they might have been transferred, and who else might be involved.

2:52 Have you done this successfully, Tom? Do you have some examples, for example, of where you successfully recovered monies from fraudsters?

3:01 Yeah, absolutely. There are many examples, each one a little bit different. But for instance, the disclosure in imposter fraud that I've recently dealt with, revealed that the direct recipients of the misdirected funds were individuals that owned multiple properties and other cash assets, and also led further onto a trail of other connected persons and entities from the (UK) Midlands right through to the Mediterranean. And all of this provided us with numerous valuable targets to pursue and recover from. But what's also interesting is that alongside this, the disclosure also revealed that there were pockets of stolen sums, going well into the six figures, still held up within the banking system, even though we'd only become involved months after the initial fraud. Now, one would think that the 'interbank recoveries process,' as they call it, would mean that these funds are returned by the banks at their own initiative after they're made aware of a fraud. But in my experience, that doesn't always happen. To get the wheels turning and secure a recovery of these blocked funds, it often takes our involvement in tracing through the layers through to those blocked funds, identifying where they are, and then using that money trail to demonstrate to the banks our client's entitlement to them.

4:33 So, I work in claims, and this sounds fascinating, but it also sounds complicated, and lengthy. I guess, for many people listening, one of the first things that they will ask is—how much does this cost? Is there a risk that insurers will be throwing good money after bad in trying to pursue the recoveries in the way that you've outlined?

4:47 There will always exist that type of risk. Fraud and recoveries are inherently speculative. But whilst I don't wish to sound like a secondhand-car salesman, the cost of the types of investigations and relief I've mentioned, are perhaps not as great as some might assume. And, certainly, over time, we've worked hard to develop streamlined processes in an attempt to keep costs down and response time swift. I have this general rule that you shouldn't spend more than 10 percent of the loss in costs, unless you've made that decision to really get stuck in and go all the way. I guess if we're talking about seeking disclosure orders, for instance, like the ones I've just mentioned, to get to the stage of making informed decisions, then I would say that you've got a threshold loss of around £150,000, below which you have to start questioning the proportionality of that investment.

5:59 Okay. So far we've focused on social engineering, which I think usually involves the payment of what I've called kind of traditional money. But what about crypto? The insurance market, as I'm sure you're aware, has lost huge sums of money in recent years in the payment of Bitcoin and other cryptocurrency following ransomware events. And there is a perception that crypto is untraceable. But I have recently heard that US authorities have seized more than $30 million in crypto from hackers linked to North Korea. We know that the DOJ recovered $2.3 million of the cryptocurrency paid by Colonial Pipeline. So, how does that work?

6:45 The position with crypto in many respects is effectively the same as with traditional currency. The key difference is the tech that's used to trace the funds and the fact that you are dealing not with banks, but with crypto exchanges. So there have been a number of cases over the last two or three years, including one of my own, albeit a different jurisdiction, that have demonstrated the willingness of the courts to grant disclosure orders and freezing injunctions in respect of crypto-related fraud, just as they would do for traditional currency losses. An example of this is the AA and Persons Unknown case, from 2019, I think it was, in which the London market insurers behind this took the pretty pioneering step of chasing down a Bitcoin ransom that they had just paid. That ransom was traced through to a crypto exchange in the BVI, and the London insurers persuaded the English court to grant a freezing injunction against the so-called persons unknown that controlled the account to which the extorted crypto had been sent and traced. So that's a good example of this all in action. I guess it's probably worth clarifying, you'll note my references to tracing stolen or extorted crypto to exchanges. And this is because private crypto wallets to which stolen funds are usually initially sent, are as many of the assumptions suggest, effectively anonymous and untraceable back to their owner. But in order to cash out your crypto back into traditional money, so, pounds and dollars, you need to go to a crypto exchange a bit like a bank or a foreign-exchange desk and convert them into traditional cash and send them to a high-street bank account. Most criminals at some point after a fraud, they do this. And that provides the opportunity to start looking at a recovery. And that's because much like with banks, these exchanges are developing increasingly strict requirements in respect of KYC and proof of identity, and also details of linked bank accounts, before you can open an account with them. So, if you can get your hands on this sort of information through disclosure orders against the exchanges, then the potential recovery opportunities really do come within touching distance.

9:36 And cost aside, are there any potential downsides? After I spoke to you, when I began just kind of discussing what you and I have talked about with others, I think there were some concerns, particularly when it comes to ransomware, that there could potentially be downsides—do you have any thoughts on that?

9:57 Yes, I think that ransomware attacks and recoveries raise their own particular issues. The key one, I would say is where the attack has involved the exfiltration of data. There may exist, justifiable concerns that pursuing an aggressive recovery strategy in respect of a ransom that's only just been paid could simply prompt retaliation on the part of the bad actors. And, in particular, retaliation in the form of disclosing the policyholder's sensitive and confidential data, which, of course, is the very thing that the ransom was paid to avoid in the first place.

10:44 Okay, so there are definitely other considerations around costs. But still, in my view, sitting here in the claims world, these are all things that should be considered. And there will be cases in which it does make sense to more actively pursue recoveries and I think the market is doing at present. On that note, why do you think it is that this isn't a route that is pursued very often in the financial lines world? In other lines of business, pursuit of subrogated recoveries or other types of recoveries, it's very, very common, and it really happens as a matter of course, but we don't seem to be seeing it so much in cyber and financial lines.

11:22 Yes, I think that's right. A big factor is potentially simply awareness of the available opportunities and remedies. As you've alluded to, the fraud-losses of the type that we've been discussing tend to hit policies that fall under that banner of financial lines, which for the most part concerns the exposure to third-party liabilities, and where the claims that arise typically require a more defensive and reactive approach. And in that sort of claims environment, freezing injunctions and invasive disclosure orders are not really part of the usual toolbox. There's probably an education piece to be had around the fact that there are these alternative legal mechanisms, processes, and supporting tech out there, when you're faced with fraud losses.

12:22 Do you think that there is more that the insurance industry can do collectively to perhaps stem the tide of the types of losses that we're talking about? Because, you mentioned the 2019 case, but I'm not hearing a lot about collective action—do you think that if the insurance industry collaborated more on these types of issues in these types of cases, we could start to see, for example, a decline in these types of losses?

12:50 I definitely think that's the case, that's a really good observation. It's obviously hard to measure the success of collective action, but I'm a strong believer that that sort of action can have a very material impact. If the insurance market were to bare its teeth and more routinely take action against the wrongdoers and their assets, and even support law enforcement to achieve prosecutions, as we've done domestically and overseas, that could have a real impact in increasing the wrongdoers' perception of the risks that they're taking in these frauds, and could well dampen their enthusiasm to be part of it.

13:33 Absolutely, Tom. Do you think that other sectors might have a role to play in any collective action, as well?

13:39 I feel that there are lots of opportunities for collaboration out there. And if we seize those, then I'm really quite positive that we can bring the fight back to the criminals.

13:49 Some real food for thought there, Tom. Thank you so much for joining us today.

OUTRO

13:49 Thanks for listening. Feel free to download, follow and share on social and recommend us to colleagues and clients. See you here next time for another Mosaic Moment.