# Operation Birks

**Host – introduction**
The Australian Federal Police – or AFP for short – is Australia's national policing agency. Its aim? To – outsmart serious crime with intelligent action. Officers from the AFP work with local, national, and international agencies to combat serious criminal threats. Their work includes counter terrorism, serious organised crime, human trafficking, cybercrime, fraud, and child exploitation. The AFP exists to disrupt major criminal operations. In 2020-21, they did that over 400 times. They seized 38 tonnes of illicit drugs and precursors, and assisted overseas police services in seizing 19 tonnes of drugs. The AFP charged 235 people with child exploitation, and charged 25 people following terrorism investigations.

The Australian Federal Police is opening its doors to give you a glimpse of how their officers investigate the most serious of crimes and stay one step ahead, to keep Australia safe.

**Host**
In recent times, Australia has had a number of well-publicised security breaches in big companies that hold vast amounts of personal information. Operation Birks provides insights into how cyber-criminals can use data from such breaches to steal millions of dollars from unsuspecting victims, and how the AFP can catch them.

**Host**
Jim is a detective leading senior constable with Cybercrime Operations at the AFP. Before Cybercrime, Jim worked in Counter Terrorism and part of his job was to track down Persons of Interest using tools that exploited open source intelligence. Doing this work led to an interest in exploring Cybercrime which was a challenge in the time of VPNs, the dark net, crypto-currency and virtual servers. Law enforcement officers needed to keep a step ahead in the virtual space. Despite not having a background in this area, Jim decided to move outside his comfort zone and give Cybercrime a try.

**Jim**
Working at cybercrime is really good in the AFP because unlike security agencies and people in the private sector at cybercrime, we get to do the cybercrime investigation. We then get to execute warrants, debrief the offenders, and actually get access to their devices. So in that regard, it's really challenging and a really good place to work if you're in involved in cyber.

**Host**
Jim started in Cybercrime in Canberra in January 2019. One of his first jobs was a referral from ReportCyber. ReportCyber, located at cyber.gov.au, is the national cybercrime reporting system run by the Australian Cyber Security Centre (ACSC) on behalf of all Australian police. Reports submitted through ReportCyber are allocated to the Australian police force with jurisdiction and responsibility for investigating them. While the frauds investigated in Operation Birks had been referred to state police, it wasn't until an analyst at the AFP examined them all together that a frightening pattern emerged.

**Jim**
We received a referral regarding a syndicate who were targeting money held in superannuation funds, and this syndicate had stolen millions of dollars from Australians in a relatively short amount of time, and it was obviously a concern to us. Now, all of these crimes have been reported to state police partners and the AFP in isolation, but it wasn't till a colleague from the AFP working at the Cyber Security Centre, looked at them all together and realised that this wasn't just isolated incidents. He realised that it was actually a serious organised crime syndicate who was targeting superannuation. And so he escalated the matter and that's how it landed with Cyber Investigations in Canberra.

**Host**
Part of the reason for the early success of the hacking syndicate was that banks were not traditionally targeted in this way.

**Jim**
Working out what they were doing was really important. I think historically, offenders didn't target banks and they didn't target superannuation companies because they were perceived to be infallible. Just too hard to get into. But technology has changed and there's a bit of insider knowledge and there's a lot of trial and error and a lot of tools out there that weren't available to cyber criminals many years ago. So all of a sudden people have started to try and hack accounts and take money from superannuation companies. And when they discover that formula, when they hit on that formula, that's basically opening the door to offending. So the superannuation companies were very keen to firstly have the offenders arrested and also to work out what their vulnerabilities were so that they could patch those vulnerabilities, which they did.

**Host**
Investigators for Operation Birks needed to identify how the offenders in this case acquired the stolen personal identification information that they used to access superannuation accounts. One common way is using IDs stolen in large-scale hacks.

**Jim**
If you have stolen identification documents, you can set up an online account within minutes. We've heard about hacks and the fact that a lot of data has been stolen and a lot of personal information has been stolen. This is how the criminals make money. So they're using those documents, the license numbers, the Medicare cards, the other documents that people have, and they're setting up fake bank accounts using phones and fake email addresses.

**Host**
The way this fraud worked was: the offenders used the dark web to buy stolen personal data, then set up fake or 'mule' accounts in which to transfer people's superannuation.

**Jim**
Initially what they were doing is they were taking that stolen personal identification information, working out whether or not someone had a superannuation account with a

particular superannuation fund. They would then make contact with the superannuation fund either through the chat function or through phone calls, and just change some of the details, like change the phone number or change the email address. They would then let that sit for a couple of weeks. They would then use the stolen identification information and put through fraudulent claims to have superannuation deposited into a mule bank account.

**Host**
Sometimes, the amounts of money going into these mule accounts were significant.

**Jim**
They had to deposit the money into bank accounts, and that's what these mule accounts were for. So they do fraudulent withdrawals from a super account, in some cases, $400,000 in a go, and they would transfer that money into a mule account. Once the money was in the mule account, they'd send a debit card offshore to a colleague in Hong Kong who would then buy electronics or jewellery or gold bullion and sell that and then return the money or the funds back to Australia as cryptocurrency that was much harder to trace.

**Host**
It became obvious to the investigators that the syndicate behind these thefts was operating on the dark net. That meant scammers from around the world were connecting with each other but only performing one component of the fraud.

**Jim**
In some cases, there were people that did the photoshopping and prepared the documents. In some cases, there would be people who compromised the computers. In some cases, there would be people who actually made calls to the superannuation funds. These callers specialise in one thing and they get a cut of the amount of money. And in many cases, the people don't even know who they are. So they agree to commit offences together without knowing who else they're in bed with. And as long as the people get paid or pay the money and get their fair share, they will continue to work with those people. So there are, for example, the person who compromised many of the computers and set up a phishing website was based in America.

**Host**
It's timely to explain here what phishing is – that's phishing with a ph.

**Jim**
Phishing is one of the evolutions in this crime type. So initially they started off with a lot of personal identification information that they had acquired from a company that had been compromised. That company also had records of people's superannuation accounts, so they were able to get the personal identification information and the details of the super accounts from the one company. But as time went on, they evolved. They got more sophisticated. So what they did was they set up a phishing website where they basically copy or mimic a legitimate website. And when the user goes and looks up that website and puts their username and password in, that information is stolen by the offenders and automatically, the victim is diverted to the actual legitimate website. So what that means is that you go to a website you think is legitimate, that harvests your passwords and then diverts through to the legitimate

website. They can then get access to your superannuation account. Once they have that access, they can do things like change the address, change the email address, change the phone number, and that sort of thing. So that's how they used a phishing site. And in this case, they actually paid for their phishing website to be promoted so that when you did a Google check on that particular superannuation fund, the phishing website came up before the legitimate website, and that was not detected at the time. So it was active for a month or so. And in that month, they got dozens of account credentials, which meant that they were able to access people's accounts. For the offenders, it was most desirous to have people who had reached retirement age because they could actually do vast lump sum withdrawals of superannuation. So that's what they were aiming for. And in many cases, that's what they got.

**Host**
The AFP often works in partnerships with other agencies. Before the superannuation fraud came onto the AFP's radar, it had come onto the radar at ASIC where Scott Bowie works as a lawyer.

**Scott Bowie**
The Australian Securities and Investment Commission is referred to in short as ASIC. We regulate the corporate sector across Australia. So we're a Commonwealth agency and we also regulate the financial markets. I'm attached to an area of that, referred to as Markets Enforcement. We are mainly involved in the regulating of the financial market participants looking for misconduct and investigating it, and ensuring that the participants comply with the Corporations Act.

**Host**
The case that came across Scott's desk at ASIC was not superannuation funds fraud. His case involved share trading.

**Scott Bowie**
Going back to 2018, retail investors, , were reporting misconduct to ASIC through the system that we have there. They were complaining of having their share portfolios stolen without their knowledge.

**Host**
With these earlier cases, investors reported their shares had been stolen then sold. ASIC discovered the money had been transferred into accounts set up using stolen identification.

**Scott Bowie**
The sales were occurring through large share brokers in Australia, and that was mainly happening through the use of stolen identification information. So the organised crime syndicates were using the stolen identification information such as driver's license, Medicare cards, all of that information that you can obtain when you hack a company and steal their HR or payroll database, that sort of information. They were using that to set up bank accounts with the stolen identification, then complete forms with the brokerage facilities to do like one-off sales of people's portfolios. And that's how ASIC then got involved because we started to obtain this information from the brokers, and look at all of that data.

**Host**
Before ASIC and the AFP realised they might be looking at the same set of offenders, Jim at Cybercrime was busy finding links between the superannuation accounts that had experienced fraud. He knew that even though the syndicate had worked out how to steal money from superannuation accounts around Australia, because of the nature of cybercrime, they could be doing it from anywhere in the world.

**Jim**
One of the challenges with cybercrime is that the offenders could be based anywhere in Australia or anywhere in the world. In the era of VPNs or virtual private networks, virtual private servers, the offenders could, and were in fact in many countries in the world. And we had no idea. Because it's so easy in cybercrime with cryptocurrency and technology to hide your location, when the referral came through to us, we actually didn't know where the offenders were, and that's why it was referred to a team in Canberra as opposed to one of the regional teams in Sydney, Melbourne, Perth, or Brisbane.

**Host**
One of the investigators at the Australian Cyber Security Centre identified 35 accounts that had been targeted at a major superannuation fund. The investigator also identified a number of bank accounts that had money transferred into them from superannuation. Some of the super fund's cyber security had worked, so while the syndicate had attempted to steal seven million dollars, they only ended up with $1.4 million because the fund had strengthened their security measures.

**Jim**
A colleague from the ACSC approached me and said, 'Look, we've identified that it's not, one offender and a couple of accounts; it's actually 35 accounts that they've tried to hack, and they've been successful in a very short time in getting 1.4 million dollars. This is not one person; this is an organised syndicate. We have to look into this.' My colleague did some really good work in identifying that it was the same people, the methodology was the same. They were using the same IP address. In many cases, they used the same fake bank accounts, and they also use JP stamps or Justice of the Peace stamps to falsify documents that are then submitted to the superannuation companies to make fraudulent withdrawals. He worked out that, in fact, it was the same group of people. It wasn't just one or two offenders who are being opportunistic. This was organised and they knew what they were doing.

**Host**
Justices of the Peace are used for the certification of some documents. The JP stamps, it seemed, were easy to duplicate. And this was necessary because in order to move money out of the superannuation accounts, the syndicate needed to set up accounts in the same names as the original accounts to avoid too much scrutiny.

**Jim**
It was virtually unheard of that people would actually be so audacious as to do this. So the superannuation funds weren't really on high alert and looking for this. So quite often, the

offenders were able to change the email address, the phone number, and the account details, and in some cases, the date of birth on the superannuation account. They had to submit paperwork to do this and they would use fake JP stamps.

**Host**
When the offenders set up fake bank accounts using stolen data, they also needed two other components. Firstly, a fake account needs a postal address. And secondly, with two-factor identification which is now widely used, they needed phone numbers for each account. With such large-scale fraud, that meant the offenders needed a lot of SIM cards which they could use in burner phones. Even though these fraudulent accounts were linked to post office boxes rather than residential addresses, this gave the investigators a starting point. Scott from ASIC explains:

**Scott Bowie**
We had analysts and investigators combing through that information, looking at the addresses listed, the post office boxes, the phone numbers provided on the forms and there was a lot of information there. From that we then identified that there was clusters of offending going on here. Ultimately there was more than one criminal syndicate that was active, and it led us to make some inquiries with a pharmacist based in Sydney. And when we made those inquiries, clearly that pharmacist had their identification used to facilitate the crime. So it wasn't actually them. It then led ASIC to make inquiries with a person of interest based in Victoria.

**Host**
After the AFP and ASIC teamed up to investigate both the share trading fraud and the theft from superannuation accounts, they got in touch with the Australian Transaction Reports and Analysis Centre, AUSTRAC. Natasha from AUSTRAC explains exactly what they do.

**Natasha**
AUSTRAC, we serve a dual role. We are a financial intelligence regulator and so what that means is we regulate the financial sector and require them to submit certain types of financial transaction reports. And we are also a financial intelligence unit and so we take those transaction reports and we analyse those for intelligence purposes. So what that means is that everyday transactions can shed a lot of valuable insights into why somebody might be moving money, or how they might be involved in something that is either unusual, suspicious, or part of a crime.

**Host**
The analysis of financial transactions is a critical part of any investigation, revealing who the offenders might be and where they are.

**Natasha**
the AFP and ASIC undertook the investigation and had a look at some of the finances and what went wrong and how, some of the funds involving the superannuation funds and share funds were moved from one account to another. And so they approached AUSTRAC at that point for some assistance with working with some of the financial institutions. And so what AUSTRAC did at that time was really drilled down into step-by-step what happened in terms of how these

criminal groups managed to gain access to customers' identification details; how the criminal groups managed to create different types of accounts, whether it be bank accounts or superannuation accounts; and then how they managed to remove the customer's funds from those accounts and then move them offshore.

**Host**
Natasha explains how the offenders moved the stolen superannuation money off-shore

**Natasha**
What was happening in this instance is that when a bank account here in Australia was being opened up using fraudulent identification details, the debit cards that were linked to those accounts were couriered overseas. And so as soon as these scammed funds would hit the domestic bank accounts, the overseas criminals were using the debit cards that had been couriered over to Hong Kong, and then being used overseas to make purchases for handbags and jewellery, luxury items that hold a lot of value. And then it was those items that were being sold.

**Host**
Superannuation funds are designed not to be accessed until retirement age. Jim explains how the scammers got around this.

**Jim**
Once these people realised that they had access to super funds with large sums of money in them, but the people weren't over the age of 60, they had to work out a way around that. So what they did was they used the stolen personal identification information and set up a second super fund. So, for example, if you're with Superfund A, which records your date of birth as being born in 1975, you might go to Superfund B and set up a superfund using the stolen identification documents that have been altered so that it appears that you are born in 1955 and so you transfer your super funds from fund A to fund B, and that means you can then withdraw from fund B. And that's something that they were doing. So it was quite complex. A lot of trial and error and once they, land on a formula that works, they exploit it.

**Host**
One of the reasons this method was really successful in the beginning was because super funds had never seen anything this audacious. Historically, their security protocols had worked, but with the evolution of cybercrime, they quickly realised that they had to improve their cybersecurity.

**Jim**
Bear in mind that this was five years ago and the superannuation accounts had never had fraud like this. Thankfully the super funds are very ~~re~~ reactive and responsive and take this very seriously. So they've now beefed up security so this is much harder.

**Host**
As soon as the fraud was identified, AUSTRAC helped the financial sector understand the patterns of offending.

**Natasha**
The AFP undertook all the investigation and they then approached AUSTRAC with, 'These are our findings. These are the patterns or the consistencies that we've noted among these cases.' And so it was those patterns that AUSTRAC compiled and then shared with the broader superannuation sector so that they were then able to look out for similar patterns. So if all of a sudden they were starting to receive an update of identification information, particularly relating to dates of birth where a JP had signed off on that change, then that would be considered a red flag or something that would generate further questions or enhanced customer due diligence checks to be undertaken.

**Host**
Working with the financial sector to reduce vulnerability was a pressing need, but finding those responsible was also a top priority. With burner phones and post office boxes, there was a lot of information that could lead investigators to the culprits. At ASIC, Scott found that one bank account was being used to finance a number of burner phones.

**Scott Bowie**
That bank account was used to recharge burner phones coz this syndicate was very good at hiding under layers of identification fraud. They used identification to set everything up so nothing was in their real name. What we needed to do was do a lot of analysis of banking and telecommunications information, also cryptocurrency transactions to try and find a lead which would lead to the real world and then identify a person of interest that we could then look at a little closer. So at that point we managed to find some banking accounts that were of particular interest, which had recharged some of these burner phones and the burner phones had been used on the application forms to commit these offences.

**Host**
While this particular offender was generally careful using different SIM cards for each account they were hacking, it only took one mishap to lead investigators at Operation Birks to her door.

**Jim**
The offender was using SIM cards and I think they put 200 SIM cards through a particular phone. And on one occasion they had done some offending, but then foolishly made a phone call to a business that would allow us to track them.

**Host**
This is more common than you might think, and we have even covered this in Season 1 of Crime Interrupted. The most careful of criminals can occasionally forget and use their burner phones to order takeaway. In Season 1, it was a ham and pineapple pizza. In Operation Birks, it was kebabs. Scott explains how one order of kebabs could bring down the house of cards.

**Scott Bowie**
We were then able to identify some particular calls of interest. One of those was to a kebab shop based in Melbourne. we thought this could lead to us identifying the real person who had called up the shop to make a order for some kebabs, and the owner of the kebab shop had

written down on a piece of paper the name of the person, the address where it was to be delivered to, and one of our investigators followed up on that transaction. And we then went down there and obtained that information and we got that person's name and address where the food was delivered. So that allowed us to then make further inquiries, look at the person, at the address, identify exactly who they were. From that, we did further telecommunications analysis of more burner phones. And what we found is the phone that that person was using in real life, they had a phone that they were using for their personal communications, and that phone worked in lockstep with one of these burner phones that had been used in some of the offending. That then cemented our case theory that it was this person who was the main suspect in the offending.

**Host**
It turned out that the Melbourne part of the syndicate was a 21-year-old woman who we are going to call Hannah. Investigators began monitoring her closely.

**Scott Bowie**
What we then did is, through further analysis, we found that the person of interest was then, making calls through a travel agency and was booking a holiday overseas.

**Host**
Once Hannah was identified, Jim and his team at Operation Birks had to find the best way of investigating her and stopping her. In the end, her overseas holiday provided the perfect solution.

**Jim**
Well, there wasn't a great deal out there regarding Hannah. We knew that she lived in North Melbourne, but she had no criminal record. She had some interesting associates, but there was nothing that indicated that she was involved in cybercrime. Having said that, the information from ASIC was very good, and that led us to progress to the next stage of the investigation, which was resolution. Now, when that happened, we had a couple of options that we needed to consider. The first is to use what we call special projects, so using technical solutions that we don't really talk about. However, that is very resource intensive and quite often, is very limited in its value. We thought about doing things like where we kept someone under surveillance, but we could be doing this for months before we actually captured the evidence that we needed to be able to prosecute. So the third option was a disruption option. We just damn the torpedoes, we roll the dice and we do a search warrant, and hope that we find enough evidence when we do the search warrant to be able to prosecute. And that is a big risk because if you go in there and you don't find what you're after, the case is blown and it might lead to you missing several other targets. So it was a big decision that we had to make as to how to proceed, what the next step was. Fortunately for us, one of the analysts from ASIC had identified, out of the blue, that Hannah had gone offshore and would be returning in three weeks. Now, that to me, was a really good opportunity to execute search warrants because she would have her devices in her possession at the time. One of the challenges in cybercrime is attribution. So you might have a computer or a phone at a house, but it's open for the person who lives at that house to say, 'Hey, that's not mine; that's my flatmate's,' or whatever. It's much harder to deny that you are in control of a phone or a computer if it's found on your person. So we made a decision to dam

the torpedoes. Worst case scenario, it would be a great disruption and a great disincentive to continue this offending. We made a decision to proceed with warrants when Hannah returned to the country.

**Host**
This golden opportunity to seize Hannah's computer and phones was an example of the good luck that sometimes comes the investigators' way. It's hard to deny that a phone and a computer are yours when you're travelling with them in your carry-on luggage. Once the investigators at Operation Birks found out the date Hannah was returning to Australia, they enlisted the help of their partners at Border Force.

**Jim**
As soon as we realised that Hannah was returning to Melbourne, we spoke to our partners at Border Force who were as usual, fantastic. They were able to pull Hannah and her devices and her luggage into a small room. And with our colleagues from ASIC, we started executing search warrants. So we were able to get access to the devices, which was very useful. Hannah, spoke to a lawyer very quickly who gave her advice not to speak to the police, and that was fine. We had access to the devices and so we were happy with that.

**Host**
The stopping of Hannah as soon as she returned to the country was the culmination of a year's work for ASIC.

**Scott Bowie**
The AFP strategically stopped Hannah when she came back into Australia, and that worked extremely well in this case. Some of it I guess, is good planning and strategy and some of it, it's a little bit of luck in these cases. But it all came together quite nicely. So, ASIC was also present. We wanted to do a search warrant at Hannah's premises but it was also extremely beneficial if we could obtain the devices that Hannah was in possession of when she came back into the country. That would allow us to then get hold of these devices, which we hoped had a lot of evidence on them

**Host**
After taking Hannah's devices for examination, the search of her home began. When the investigators first entered the house, it did not immediately look like the house of someone steeped in cybercrime activities.

**Jim**
When we walked into the house, it was very neat, and initial inspection, we didn't find anything that would suggest that this house was used for cybercrime. There were no computers. There were no devices. There was nothing other than what we actually found on Hannah at the time of the warrants. However, when we walked in, we noticed a couple of things. The first was a big box of SIM cards, hundreds and hundreds of Optus SIM cards, and many of those SIM cards had numbers and names written on the labels. So that was the first clue that we were on the money. We also found on the desk, a box of gloves. So the gloves were used to prepare the documents that were then sent to the super funds to make the fraudulent withdrawals. And this

was consistent with what we knew because we had fingerprinted and done DNA testing on the documents that had been sent in, and they all had smudge marks and no fingerprints. So that was consistent with gloves being used to prepare the documents. Something else that we found on the printer was a withdrawal from a particular super fund for several hundred thousand dollars in the name of Neil. And that was already in train, so that was sitting on the printer. And that is something that Hannah had forgotten to take off the printer and dispose of before she left. It appears that she left in a rush, as we all do when we go to the airport and she sent a text to a friend saying, 'Look, I really need you to do me a favour. Can you empty the bins?' While the friend never got around to emptying the bins. By the time we went through the door, and in the bins, we found loads of documents that had been used to defraud numerous superannuation accounts. So much of the evidence that we found, in fact, was in the bin. And if that had been taken out on the day we never would've found it. So that was a bit of a coup for us. It also speaks to the fact that if we do search warrant, we search everything, we take everything to pieces, absolutely everything. And I think the searches took 20 hours on that occasion.

**Host**
It is common for online scammers to use encryption software to communicate with each other and this is what the investigators found in this case.

**Scott Bowie**
At the search warrant at the premises, it was a treasure trove of evidence for us. Not only was there documentation related to the offending inside the premises, including SIM cards, which were used in burner phones, but there was also some documentation which had a fingerprint on it, which was in the rubbish bin. It certainly paid dividends to be thorough, and the AFP did a thorough job in conducting the search and seizure at the premises. We also had the good fortune of digital forensics and they were very experienced, so they were then able to access encrypted telecommunications between syndicate members using like the encrypted apps such as Telegram. There's a number of these different communication apps out there, but in this case, Telegram. And then download those communications, which was extremely beneficial for our case because ultimately, we ran a case of conspiracy. So we needed to show the different roles the different people were playing the acts, which contributed to the ultimate offence.

**Host**
Hannah's devices turned out to be a treasure trove.

**Jim**
We found a lot of stolen personal identification information. We found access to dark net marketplaces that Hannah was using. We found cryptocurrency accounts. It was about 2am by the time we actually managed to get access to all of those devices. And I remember once we did get access and we could see those Telegram accounts, the dark net interactions, the cryptocurrency. It was a really nice moment in the investigation. 3am very tired. I think we'd all worked for about 15 or 20 hours by that stage, but we got what we needed.

**Host**

The investigators were able to track Hannah's communications with other members of the syndicate. Information such as this helped them see how these alliances worked.

**Scott Bowie**
It was interesting to see that Hannah appeared to meet some of these co-conspirators through forums and also through the dark web marketplace that she was operating. So Hannah was not only involved in assisting with the defrauding of people's share portfolios and superannuation funds, but also in dealing in identification information on the dark web. So how that works is other persons who are interested in buying identification information and then using that to help facilitate frauds and those types of offending, they'll go onto the dark web and source that information and pay for it. She's then connected with other persons who are interested and also involved in operating on the dark web. And then through the forums, they then connect and source different skill sets which can help them commit the crime. So one example of that would be, at some particular point, they decided they wanted to make a website that basically looked identical to the real website of a superannuation fund. And they recruited into the syndicate a person who had that skillset to design a website that basically looked identical to the website. They then, obviously, were in control of that website, and then every member who was tricked and went to that website, they put in their login details and member information, password, and the criminal syndicate then harvest a large database of that information, which they then used to access that person's member account through the legitimate website. So, yeah, at different points they're reaching out and connecting with different members who could assist them in different aspects of it. Another aspect would be the laundering of the money that they've stolen. They genuinely needed to get that out of a bank account that was held in Australia, and then they would launder the money overseas, say in Hong Kong. And they'd use somebody over there; post bank account information over to them and then they would then go and remove the money from the accounts using debit cards and buying large items or expensive jewellery. It was interesting from that perspective because these syndicate members may not have ever met each other and probably didn't necessarily know what each other looked like or their real name. They all had a different alias, such as Binja Bob, H, Money Monkey, that's just to name a few. But they all had these different names and they operated like that. I guess it helped them avoid being easily detected by law enforcement.

**Host**
After the arrest of Hannah and the examination of her devices and home, the investigators of Operation Birks had to put the case together for court. One of the more complex jobs was to piece together just how much she and her syndicate had stolen.

**Scott Bowie**
The amount of money, it's hard to be absolutely certain because we were mainly focused on pulling a brief together against Hannah. So we are mainly looking in the offending relation to that, but certainly a lot,. So they don't just do share sale frauds and superannuation. They're also committing frauds on people's credit cards, potentially taking out loans in people's names without them knowing. So there was a lot of offending, but we had to really scope it in so we could get an outcome in relation to Hannah. Look, you're talking into the tens of millions of dollars of money that would've been targeted. They don't get away with all of that because some of that gets stopped by the banks if it's identified as a suspicious transaction or if say a

victim rings up and says, 'Put a hold on the money.' Or if one of the share registry superannuation companies uses some of their cyber resilience type of software there to identify that the money that they're trying to transfer out of superannuation is suspicious, and they'll put a stop to that and make further inquiries.

**Host**
Even though Hannah was arrested after she returned to Australia, she was released while the investigators put their case together using the huge amounts of data they found in her devices.

**Jim**
Hannah was arrested at the time, but we had no reason to keep her in custody. It wouldn't have been fair to her, and it would've meant that the clock starts ticking, and we have about six weeks to go through terabytes of information, which plainly we couldn't do. We had to make inquiries with all the super funds. We had dozens and dozens of victims. We had to get statements and we couldn't have done that in six weeks. So Hannah was released from custody that evening. We were very confident that she wasn't gonna travel anywhere. ASIC used their powers to ensure that her passport could not be used to travel and we had to hold off. We had to get the brief of evidence done, but we couldn't get through terabytes. So Hannah was released and we went about collecting all the evidence and going through terabytes of data which we duly did. So I think Hannah was arrested in April, 2019, and we had enough of the brief prepared by about September. So at that point we went back and arrested her and took DNA evidence and charged her with the offences and served the brief on the defence. The thing that really got us was, initially we were dealing with one superannuation provider and also one share trading platform. Once we went in the door, we realised that this wasn't just one superannuation company, it was about half a dozen and we realised the magnitude and the scale of this offending. When one superannuation company detected the offending and put the roadblocks down, they just pivot to another superannuation fund or share trading fund.

**Host**
The case went to trial and in the face of overwhelming evidence against her, Hannah pleaded guilty to three charges: conspiring to defraud superannuation funds; conspiring to defraud share trading funds; and conspiracy to deal in proceeds of crime to the value of more than $1 million. In December 2022, she was sentenced to five years and six months' imprisonment with a non-parole period of four years.

**Jim**
Shame of it is that Hannah was pretty bright. She was pretty articulate. She was quite motivated. She took the initiative. If she'd gone into the private sector, she'd have made more money in a couple of years than she could make from these scams. But now she's in jail.

**Host**
Despite the amount of money stolen by the syndicate, because it was shared out, Hannah did not grow rich from her crimes.

**Scott Bowie**

Hannah was working this almost like a full-time job and the amount of money that she earned from this was in all account not that significant considering the risk. And I don't really think she weighed up the consequences and risk of getting involved. It was a slippery slope and she became more and more involved into a point where she became a key player and ultimately that was illustrated in court. And she ended up with a significant term of imprisonment. I guess if it wasn't for the mitigating circumstances that were taken into account then she would've ended up in jail for a even longer period of time.

**Host**
Natasha from AUSTRAC says that wherever there are large sums of money, scammers will target it.

**Natasha**
What we tend to see is that wherever there is money that is available for example, the large amount of money that's contained within our superannuation funds, approximately $3.1 trillion dollars, wherever these funds are available, that is where the scammers will start to target.

**Host**
Given that Operation Birks uncovered a syndicate opening false bank accounts in order to syphon money out of legitimate superannuation funds, AUSTRAC was able to pass that intel on to the finance community. When a customer changes their address, phone number, and email address, it should be a red flag.

**Natasha**
If you think about your own personal bank accounts, it's rare that you would change your phone number, your email, your address, even your title or part of your name all at once. If you are moving, you would generally only change or update your address details and everything else would tend to stay the same. If you change your phone number, everything else would stay the same except for that phone number. So if there is a customer that has opened up an account, or even multiple accounts in a short period of time, and then at the same time, updated their address, their phone number, their email address, and even removed a previous phone number or previous device that's connected to their online account that could potentially point to identification takeover.

**Host**
The investigators in Operation Birks found the financial institutions were more than willing to accept their advice.

**Natasha**
No finance provider, no financial institution wants their customers to be scammed. , I think everybody's doing their best to protect their customers. And so if there is any way of ensuring that that doesn't happen, then generally we find that, yes, those that we work with, the different financial institutions, the different banks, they are certainly willing to do what they can to protect customers and to protect their customers' money.

**Host**

As with so many of the cases we have covered in Season 2 of Crime Interrupted, it is the combined powers of a number of different agencies that allow the AFP to successfully target and prosecute those who commit crimes.

**Natasha**
The AFP or AUSTRAC, or ASIC, they each have access to different types of information. They've each got different remits in terms of their purpose. And so it's sharing all of that information together that allows you to really see the extent of a crime or a problem that is occurring. Sometimes from AUSTRAC's perspective, you can only see a portion of that crime, but by sharing all of our information together, it provides you with a clearer picture.

**Host**
While some people dabble with the dark net for fun, the minute they cross the line, Operation Birks is a good reminder that Australian law enforcement has a powerful team behind it.

**Jim**
It's one thing to get access and to be mischievous and use the skills that you have to test yourself. It's quite another to use those skills to steal from other people. And that's where it really kicks up another notch. And that's what happened in this case. That's when it's taken very seriously. That's where you have resources like the AFP, ASIC, the Cybersecurity Center, and Border Force pulling resources to go after you.

**Scott Bowie**
What we've shown is that even with an extremely complicated, sophisticated organised crime syndicate and the way they operated from different areas of the globe, hiding under technology and a lot of fake accounts, it can be thoroughly investigated, and ultimately we can identify the people and hold them to account. So if they think that they can hide out there and target Australia or particular areas of Australian industry, then they need to know that we can get to the bottom of it. We do have the capability and working with our partner agencies we can ultimately put briefs together and put people before the court, successfully prosecute them.

**Natasha**
We've got law enforcement and intelligence agencies working together with the financial sector and the superannuation sector to protect customers, to protect customers' money. All in all, it's the government's key priority to protect our community.

**Host**
Jim has a final word for anyone with the skills demonstrated by the offenders in Operation Birks.

**Jim**
It's so highly sought. We can't get enough people to help us with these investigations. Yeah, you could go down the path of the dark net. Reality is you're gonna get caught. But if you use your skills to become a penetration tester or work with authorities or the banks or whatever, you're gonna make a lot more money, you're gonna have a far easier life, and it's gonna be really rewarding. I love what I do and there's no reason why people with those technical skills

couldn’t land in a job where they’re targeting hackers to prevent this sort of thing. That’s the flip side. That’s what you could be doing.

**Host**
Since Operation Birks, the AFP, ASIC and AUSTRAC have continued their work with the financial sector to strengthen their cyber security and ability to detect and disrupts scams targeting their customers.

If you are interested in learning more about how the AFP works to protect Australians against cybercrime and fraud and how Jim, Scott and Natasha investigated this case, visit a-f-p-dot-gov-dot-a-u

**Host** AFP outro
The AFP is all about protecting Australians and Australia’s way of life.

Stay tuned for the final instalment of this season of Crime Interrupted, as we take you behind the scenes of an international drug smuggling syndicate.