2100 words

Q. Why don't you introduce yourself and tell us a little about your work and career?

A: *I have spent most of my life in academia, with several years of experience in an IT company as well. My first degree was in Physics at the University of Crete and then I did my MSc and my PhD degrees at the London School of Economics on Anti-Money Laundering and Information Systems. I'm currently a Senior Lecturer at Hull University Business School and a Visiting Professor at Texas A&M University. I'm co-chair to the International Security Conference taking place in Las Vegas annually, where we have regular participation from the FBI and the US Secret Service, and also a senior editor at the Journal of Information Systems Security. I work on the information systems management end of the spectrum so I am more interested in the organisational challenges that technological deployments create, as well as the broader systemic and socio-economic issues they place onto the world around us.*

Q. Let's start with the basics: what is money laundering and why is it necessary from a criminal's perspective and unwelcome from a societal perspective?

A: *Money laundering is typically thought of as a 3-stage process:* ***placement*** *(where the 'dirty' money enters the financial system),* ***layering*** *(where the money trail becomes complicated), and* ***integration*** *(where money is re-invested into criminal activities or siphoned into the legitimate economy). From a criminal's perspective, it's necessary because all crime generates illicit money/assets. Laundering these assets allows criminals to enjoy the benefits of the formal financial system and move money around with ease. From a societal perspective it's considered to be unwelcome because money laundering remains the main avenue through which crime is allowed to remain profitable and reinvestments in crime lead to further predicate offences (drug & human trafficking, corruption, tax-related crimes, to name a few).*

Q. Do we know how much money is laundered internationally each year? How big is the problem?

A: *No, not really. There are some figures that are circulating here and there and claim that it's the world's 3rd largest market with about $2trillion annually but they cannot stand against any serious scrutiny due to the underground nature of the phenomenon, statistical distortion of indices, and many other problems. In my book (Technology & Anti-Money Laundering) I have a small section dedicated to that problem and go through the rationale of abandoning such estimations.*

Q. Can you give us an overview of anti-money laundering. What are the key tenets, processes, cogs and wheels in the UK's anti-money laundering system?

Q. And, within the banking system – can you give us an overview of 'suspicion and suspicious activity'? Who, within a bank, is responsible for raising the alarm? And, what happens after the alarm has been raised? (I guess, in short: how do SARs work… Indeed do they work: https://www.lexology.com/library/detail.aspx?g=05e3220a-7918-4058-9f83-fa3a17673d6e)

Within banks, 'alerts' are raised by either automated transaction monitoring systems that simulate money laundering behaviour and capture them in SQL-style queries with thresholds, risk-scoring techniques, etc., or by staff members that might observe unusual behaviour or patterns of transacting in branches. Transaction monitoring systems work poorly with very low true positive rates (anything from 0.1% to 20% though these are again problematic/plasmatic and often 'gamed' statistics from banks that want to appear compliant). In any event, an alert is evaluated by ML-analysts and then if suspicion is 'confirmed' (by 'confirmed' I mean a consideration that is worthy of further escalation and not actual ML), then the bank's MLRO (Money Laundering Reporting Officer) will report the SAR to the Financial Intelligence Units. Over decades, all FIUs globally have amassed scores of junk-SARs, a tiny % of which are actionable and an even tinier percentage have led to some asset confiscations. The German case where the Criminal Law enforcement authority raided the FIU is ample evidence that the broader system has lost the plot.

Q. Let's create scenario: Criminals have used social engineering via email and voice to defraud a prospective house buyer. The criminals impersonated a solicitor and persuaded the victim to divert £250,000 in funds away from the real legal firm's account and into their bank account.

a. How will criminals likely try and launder the stolen money? What's a common step-by-step approach?
b. Where in the process are the criminals most likely to get caught?

A: *There are so many combinations that we couldn't really exhaust them. The step-by-step approach would typically conform to the placement/layering/integration model. The FATF has a published list of all the different ML typologies identified but these change and new techniques develop all the time. I'd say that placement and or early integration stages are the most vulnerable stages of the process where criminals are more likely to get caught.*

Q. Looking at cybercrime again. If I want to steal your TV, I've got to come from to your house. If I want to empty your bank account, I can do it from anywhere in the world. Is there a relationship between where cyber criminals choose to base themselves and the existence of comparatively weak local law enforcement?

A. *Yes, based on my interview with Brett Johnson (a.k.a. the Original Internet Godfather) which is freely available here, but also the broader cybersecurity literature, one can find examples of how geopolitical considerations reflect operational decisions of cybercriminals. For example, if someone is physically based in the US, they will operate through VPNs hosted in Russia due to the tension between the countries. You can generalise from that and observe the possibilities for cybercriminals to take their own operational security decisions and explore what countries do not have an extradition treaty with their home country, or look at ways to consider the weakest cybercrime policing regimes available and operate (remotely) from there.*

Q. What is a money mule and are there other ways the public can be unwittingly tempted into helping criminals launder money?

A: *They tend to transfer money that originates from predicate offences (e.g. drug trafficking, human trafficking, etc) through their bank account in exchange for a commission or cash offers. Then they transfer the money to other accounts so they participate in the placement/layering phases depending on circumstances. People in need of money, students, anyone really can be approached and they may not understand they're being used in this way (but don't be fooled by easy money – if it's too good to be true then it is). Even worse, once deceived, they will be threatened and continue to be exploited, unless they manage to break that circle and ask for help.*

Q. Talk to us about AI's place in AML. AI can spot cancer more accurately than some human doctors and it can *almost* drive a car. Would we be right to think AI might offer a silver bullet in the fight against financial crime? Or is (international) AML so complex that it is hard to compress it into something AI can manage / be expressed algorithmically?

A: *Actually, I'm hosting a workshop on AI/AML at Cambridge University in September at the Cambridge International Symposium on Economic Crime so if anyone is interested in that they can find us there. A few companies that are working in this space are also participating. Onto your question, I don't believe there's a silver bullet and despite the whole AI-excitement, human behaviour cannot be predicted, no matter what sophisticated technology we impose upon it. AI advances in radiology for example are using imagery to detect abnormal characteristics and rely on image recognition and machine vision. This is realised more easily than inferring suspicious behaviour. At the core of this problem is the following: suspicious behaviour is a subjective construct. We cannot expect AI to convert something subjective into something objective. But overall, here's how I see the scene of AI in AML: supervised machine learning is problematic as the 'truly suspicious' cases (if there's such a thing at bank level) are so few when compared to legitimate transactions so we get a gross imbalance problem in the learning algorithms. In unsupervised machine learning, we have deeper/legal/ethical problems – how were the data sorted? Can we audit/reverse-engineer the black-box or are we allowing it to flesh out suspects on its own? This kind of approach might work in fraud where outliers are way past the normal activity levels but money launderers try to blend their activities and look as close to normal as possible. In semi-supervised machine learning (e.g. active learning) we have an AI-expert systems type of combination and some interesting graph-theory based labelling approaches but my concern there is that the learning algorithms simply (re)present what the experts have already classified as suspicious so the enhancements we're seeing in True Positive Rates are rather expected and artificial (sic!). I think Natural Language Processing has interesting potential in tapping into text-based suspicious descriptions (e.g. SAR narratives) and FIU/AI deployments that could link cross-bank intelligence might see interesting applications down the line.*

Q. What about crypto currencies? I've sold my crypto currency of choice and have a huge amount of money in my exchange account. How do UK retail banks feel about accepting that cash into their network? (The pseudo-anonymity of crypto currencies must make proving money's provenance very hard?) (https://www.theguardian.com/technology/2021/apr/21/natwest-will-refuse-to-serve-business-customers-who-accept-cryptocurrencies) Crypto feels naturally suspicious!

A: *The cryptocurrency related discussion is a complicated discussion. I run a private Blockchain Forum that is business oriented and where we host several academic and non-academic speakers. My experience so far sees views from polar opposites, the crypto-enthusiasts and the crypto-sceptics. Such is the fate of all (relatively new) technologies of course, however we should also remember that the ideas for distributed ledgers (cryptographically-backed too!) go back many years and the idea that it's a new technology is a myth (as my good friend Prof Michael Mainelli and current Sheriff of the City of London writes here). Cryptocurrency-related transactions are a droplet in the ocean of*

financial transactions in the global financial system. I understand the reaction that it might feel naturally suspicious because everything 'new' is looked upon with some caution. However, that reaction is irrational. Like any instrument, the duality of good/bad is subjected to further differentiation (it is user-dependent and observer-dependent). Also, blocking an avenue of transacting altogether is actually counterproductive to AML as it drives the demand for other ways of transacting, optimisation of much more privacy-friendly cryptocurrencies than Bitcoin, cold-storage of cryptocurrencies, etc. Ultimately, it drives the financial activity to institutional arrangements that cannot perform the same money laundering detection analyses (not that those that we've got at the moment work well – they are marred by very high False Positive Rates). The more interconnections/anchors/links we have between the crypto-world and the formal financial systems, the better we can monitor it. Overall, what Natwest and/or others are doing here is simply a form of de-risking.

Q. Flipping the question on its head: is the AML community exploring blockchain as a means of reducing suspicion around transactions and chains of transactions?

A: *This is a most vibrant and developing ecosystem. Some companies are specialising in blockchain-analysis for cryptocurrencies where the ledger is public (like Bitcoin). They claim some successes around tracing cryptocurrencies and visualising/exploring the money trail that could assist the authorities but I'm not particularly convinced of their eventual effectiveness in approximating the holy grail of AML (i.e. successful prosecution of cases and asset recovery). One case that I've followed closely and in which many agencies were involved, ended up being dropped due to its complexity. In it, a handful of bitcoin wallets that had in excess of £50m inflows most of which were deemed to be associated with ransomware attacks, and ended up being linked to thousands of IP addresses involving 30+ countries. Pursuing such a case would require plenty of resources but more importantly, time! And during that timeframe, the money trail can become progressively more complicated. Even then, and even when telecom disclosures (following legal processes) allow the association between an IP address and a physical address, we might still have an attribution problem, not to mention the digital forensics challenges there. With the changing nature of money, I have long predicted a private cryptocurrency designed for and used by cybercriminals instead of one that is simply appropriated by cybercriminals.*

Q. [If you've a new book coming out or would like to us to mention your existing books, please add in: Q. Where can we read more of your work and ideas?]

A*: My books can be found here . One is published by Edward Elgar and titled Technology and Anti-Money Laundering and the other one is published by Bloomsbury and is a more philosophically-oriented book around the paradoxes of science and entitled Science's First Mistake. The latter is also available as a free pdf download with a Creative Commons license.*

Career questions (these need be only very short replies!)

What would you say to somebody considering a job in AML?

A: There are plenty of options in banking but not only – different industries (e.g. insurance, real-estate, etc) are subjected to AML regulations. Pro tip? Specialise in AML for casinos and then move to

Las Vegas. E-mail me when you get there so that we can invite you to our local conference and our AML panel for casinos.

What are the career pathways into AML?
The International Compliance Association has a pretty comprehensive list here

What's the best way to launch a career in AML?
Look into part-time Analyst/Compliance Audit assistants, etc., and take it from there. Plenty of IT companies or IT/consultancies are working in this space so you could join one of those.