BEST PRACTICE

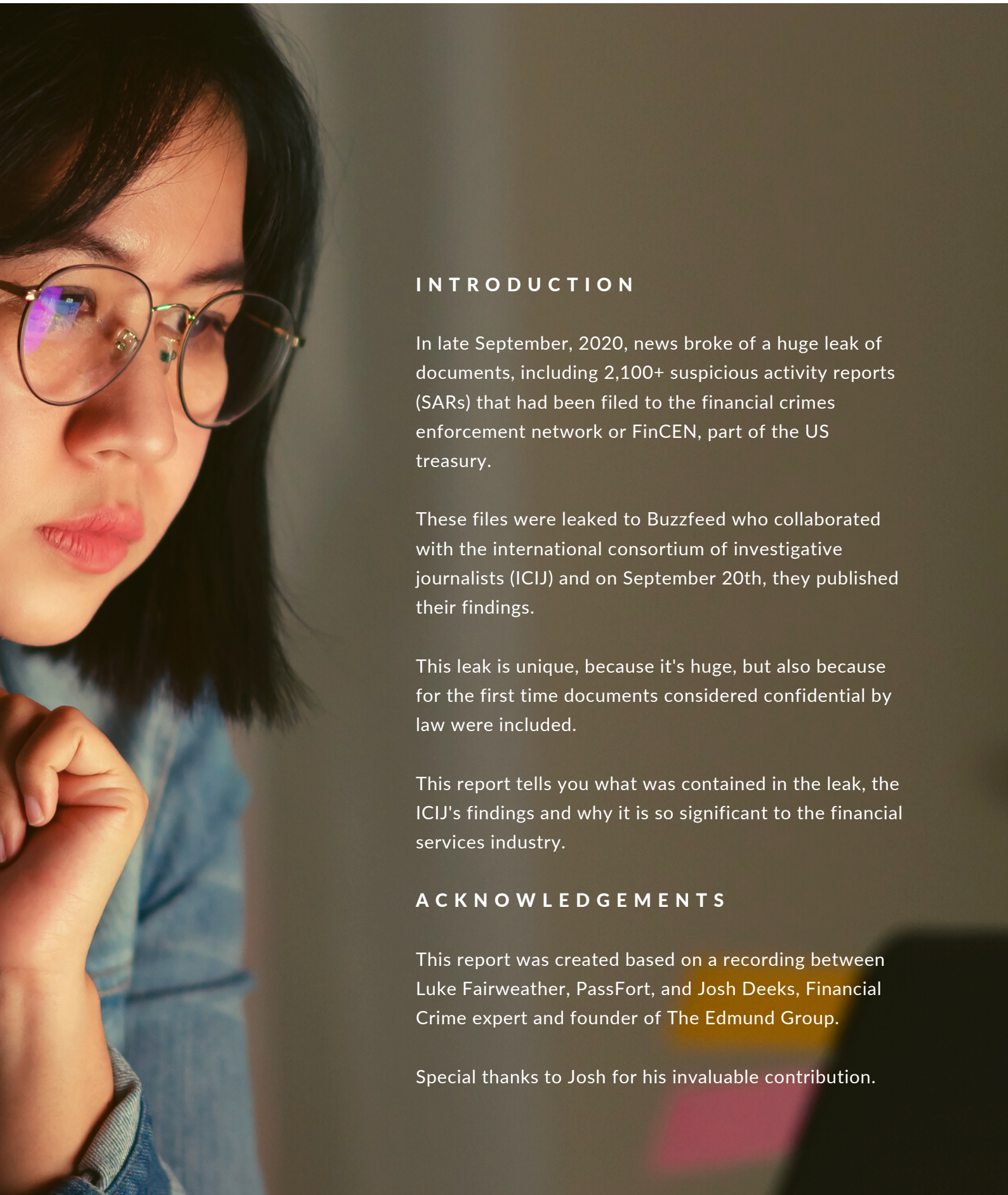
LEAKING OF THE FINCEN FILES

REPORT

PassFort

Edmund Group

Compliance. Risk Management. Anti Financial Crime.



INTRODUCTION

In late September, 2020, news broke of a huge leak of documents, including 2,100+ suspicious activity reports (SARs) that had been filed to the financial crimes enforcement network or FinCEN, part of the US treasury.

These files were leaked to Buzzfeed who collaborated with the international consortium of investigative journalists (ICIJ) and on September 20th, they published their findings.

This leak is unique, because it's huge, but also because for the first time documents considered confidential by law were included.

This report tells you what was contained in the leak, the ICIJ's findings and why it is so significant to the financial services industry.

ACKNOWLEDGEMENTS

This report was created based on a recording between Luke Fairweather, PassFort, and Josh Deeks, Financial Crime expert and founder of The Edmund Group.

Special thanks to Josh for his invaluable contribution.

JUST WHAT DID HAPPEN?

Josh Deeks: Essentially, there was a leak of 2,657 different documents, including 2,100+ suspicious activity reports (SARs) filed to the FinCEN between 1999 and 2017. FinCEN is the financial crimes enforcement network, part of the US treasury.

These files were leaked to Buzzfeed who then collaborated with the international consortium of investigative journalists (ICIJ). On the 20th September, they published the output of this investigation. This leak is unique, not just because it's huge and there's lots of data, but for the first time, documents considered confidential by law were contained in it. We are talking about the SARs.

This gives us a view of exactly how and when the banks in question identified the SARs, what they did thereafter and how they continued to behave and manage relationships. The report also details how they reacted in response to law enforcement, when law enforcement came back to them on the SARs.

There has been a huge amount of press interest, particularly because it surfaced to the public eye and I, for one, think that's a good thing.

Financial crime is a huge global problem and it is great the public is now more aware of it.

Contained in the investigation were truly significant things. The headline figure is that $2trillion of illicit money has flowed through various banks.

To break that down and put some context around it:

- 400 journalists went through more than 22,000 pages of information
- In those 22,000 pages of information were more than 10,000 different subjects and by subjects we mean individuals, companies and property
- In terms of money flow, there were 170 countries involved and there are only 195 distinct countries in the world right now
- The vast majority of the world has been involved to some extent

The statistics do a number of things, including showing the scale of the leak and the size of the problem.

There were a lot of people involved and the sheer scale of the leak and its reporting are quite something.

HOW FRAUDSTERS EXPLOITED THE SYSTEM TO MOVE MONEY

Josh: There's a lot of financial criminals in the world and they are smart people. They know tax laws inside and out. They know corporate structures and legal entities inside and out, and they help enable the system to move. They structure companies and create corporate structures to hide who the ultimate beneficial owners of these entities are.

The UK corporate system is one of those that is, unfortunately, useful for a criminals to exploit. In the centre of most of the money laundering cases, especially the major ones, you see UK companies. It's global partnerships, not always offshore structuring that causes problems. The issue can be right here in London or the UK itself.

Luke Fairweather: Do people tend to choose the UK to add a level of credibility or legitimacy to their operation?

Josh: The UK is considered one of the financial hubs of the world, so if you have a company that's incorporated in London or the UK, generally it does bring confidence to others around the world.

Let's not forget, a lot of the companies used for money laundering have business engagement that's nowhere near the actual income they are generating. The majority of that income is going to come through financial crime, but all of them will have some form of presence in a legitimate operation.

There's a good point to make about being incorporated in the UK and that providing a degree of credibility as a business, but also it is really easy to incorporate a company in the UK. It's easy to use our corporate structure to create companies and move money.

I opened the Edmund Group in March 2020 and it was done in 10 minutes. There were almost no checks on who I was or who I was planning to create this business with.

The process is slick and easy, which is great for business enablement. It's great for commerciality, but it's also pretty good, unfortunately, for opportunists that want to use it for elicit purposes.

"In the centre of most of the money laundering cases, especially the major ones, you see UK companies."

EXAMPLES OF SCHEMES IDENTIFIED IN THE LEAK

Josh: The FinCEN files allege multiple accounts of fraud. There are 5 very large-scale frauds that are noteworthy. For instance, they allege HSBC approved the transfer of tens of millions of pounds in funds, linked to the “WCM 777” scheme, which is a well-known investment fraud.

It was a classic Ponzi scheme. The story goes - invest in this bank; it's going to be great; you'll get returns; and if you seek other people to invest in our scheme you get even better returns. But, the whole thing is fake.

The reason this case is noteworthy is it was tied to a tragic death. A 44-year-old was beaten to death because he fell victim to the scheme. He encouraged other people to join, which they did and they subsequently lost lots of money and they came for him.

Luke: When you think about the vast numbers, not just in terms of the SARs, but the scale of the money at hand, $2trillion is incomprehensible, but it's so different when you put the human face of suffering on the situation.

Josh: This is the thing we want to bear in mind, especially financial crime and compliance professionals. Sometimes it's easy to get wrapped up in the bank statements we see day in, day out, and the transaction monitoring reports. Those are actually just the backend. That's not the real reason we do what we do. We do it because people fall victim to a fraud. People lose money. Some people lose their lives.

Luke: You were keen to draw attention to a second case, which was One Coin.

Josh: This one is more my own personal fanboying because I like the podcast. For anybody who’s a fan of the Missing Crypto Queen podcast by Jamie Bartlett, the FinCEN files draw reference with money moved in relation to the One Coin saga.

The Missing Crypto Queen podcast is a fascinating and concerning story about Dr. Ignatova who founded One Coin, which ended up being one of the largest cryptocurrency scams we're aware of to date.

"The FinCEN files allege BNY Mellon allowed the transfer of $137million connected to One Coin to proceed."

I gave a little information about how the previous investment scheme worked for WCM 777, One Coin is not entirely different.

It simply encouraged people to buy One Coin to inflate it's price. It got absolutely huge and then Dr. Ignatova disappeared. The podcast is about trying to find her.

Even if you're not a financial crime professional, I'd definitely recommend it.

Luke: It's probably part of the reason there's still an element of hesitancy around crypto. FinCEN does go to show that real money is just as risky as crypto though.

Josh: With any currency (cryptocurrency or otherwise) or any kind of asset, you're always going to have fraud. You're always going to have those seeking to exploit it.

I agree, there's still hesitancy around cryptocurrency arising from the types of issue characterised by the One Coin fraud. Fake ICOs (initial coin offerings) are huge issue that needs to be dealt with. But crypto is the same as most other change in finance - you have to gain confidence and once you have, the "product" becomes widely used.

Luke: Regulating crypto is a big issue in AMLD5 and 6, but with such stringent regulation already in place, particularly around anti-money laundering, could you give insight into how the activity was allowed to come about?

Josh: Financial services is one of the most regulated markets in the world. There's not much that's more regulated than financial services other than medicine and food.

The leak alleges basic AML failings. I say basic, but getting it right is actually difficult. The files allege things like due diligence, either onboarding or throughout the relationship, was found wanting.

- Institutions didn't know the true origin of the funds they were allowing to be transferred
- They didn't understand where the funds were coming from, but they were moving them anyway
- They didn't understand if the customer should legitimately have the level of money they had and should be receiving the level of money they were receiving
- They didn't know if people should have been sending money to the places they were sending it

"There were failings in gathering basic information that one would reasonably expect to be there."

In the cases that involve transactions where there were shell companies or shelf companies, the files allege that banks either failed to identify the true beneficial owner or simply didn't take a sufficiently deep investigation.

For example, JP Morgan Chase allegedly failed to identify a man who was accused of being in the Russian mafia's boss of bosses. He was supposedly on their books for more than 5years. At one point, this chap was on the FBI's top 10 most wanted list, so it's unbelievable that you could have this customer and companies associated with this customer on the books.

We see from the leaks more than $1bn was transferred in the duration of his connection to the entity. This is something you'd expect at first media screening, onboarding, adverse media screening and at appropriate times through the duration of the relationship to be picked up. Given the likely risk outcome of assessing this customer, reviews should happen frequently.

Even if there were no reports at the time he was onboarded, or his associated entities were onboarded, issues should have been found during the relationship, and it certainly shouldn't have lasted 5years.

In other cases, the legal legislator, the banks themselves didn't find out that the party to a transaction or the transaction itself was deemed capable of being suspicious until after the fact. What I'm saying is the transactions occurred, then through some form of information the bank decided to take a look back at the transactions and realised with hindsight they were indeed suspicious and should be reported.

HOW SHOULD REGULATORS RESPOND?

Josh: By its nature, regulation is typically reactive. We see regulation change and regulatory reforms when something has already not worked.

In the past was the financial crash of 2007 / 2008 and then we saw widespread reform on capital and liquidity requirements. This is the stimulus that typically engages regulatory attention.

We will be looking at reforms and amendments to the rules that exist today. The standards and expectations have to go up. The report highlights that regulation still doesn't work, even with those who are making their best efforts, those efforts are not good enough.

For those who aren't making enough, there needs to be more stringent punishment. As an example, in Germany the maximum fine that can be levied is €10million for money laundering offenses, and that can only be levied to corporate entities, so no criminal charges can be filed against individuals. If you look at that regulatory approach, for most of the institutions we see named, Deutsche bank for example, that is nothing – it's a drop in the ocean and almost no disincentive at all.

"There has to be regulatory reform, both on expectations and punishment. Having had full accountability personally in previous roles, I still think there needs to be stronger disincentives."

If we look at the leak from the US treasury report, it had a damning assessment of the UK's approach to financial crime prevention. It compared the UK jurisdiction to Cyprus, which was historically a notorious jurisdiction for money laundering.

The assessment from the US treasury is in stark contrast to the FATF (financial action task force) evaluation report from December 2018, who praised the UK for having a well-developed and robust regime. They commented particularly that the UK is a global leader in promoting corporate transparency and having a good understanding of money laundering and terrorist financing risks posed by legal persons and those arrangements.

The reality is, all major and minor laundering scandals in the past decade have had financial flows through the UK. All exploited the UK company structure and processes.

Luke: Do you think banks will hold their hands up and say we shouldn't have done this?

Josh: We've already seen some of the responses to the FinCEN files. Buzzfeed, among the series of reports they produced, showed one which was the responses from the banks, so we already know to some degree what they say. The vast majority of them are saying they comply with their regulatory and legal obligations in full.

Some are talking about the fact these files run from 1999 to 2017, and a lot have been undertaking remedial actions since then in connection to other money laundering issues they may or may not have had. They are saying they have been leading large-scale reform programmes and those are underway and having a positive effect.

Do I think anybody's going to come out and say we made a mistake? Unlikely. Should they is an entirely different question.

Personally, as a financial professional, this reignites the flame to do better, to do more, to be more diligent and robust. Whenever we go through these investigation processes, to ask is it enough? Do I have enough information?

We have to go back and revisit the fact some funds filed SARs completely defensively. They are concerned about the fact there's an offense for not having reported, so rather than digging deep and understanding the substance of their suspicion, the substance of the individuals and presenting well-structured information, the SAR just goes in.

Saying that, the issue generally hasn't been with financial crime and compliance professionals. We have a code of ethics that requires high standards of integrity.

Luke: That speaks to the letter of the law versus the spirit of the law. Is compliance a box ticking exercise or is it something ingrained in a financial institution or a bank? Is it in the culture at the heart of the bank?

"Is there anything banks can and should be doing now following this leak?"

Josh: The leak gives us a lot of data we didn't previously have, so the first thing to be done is go back and look at the customer base and say, is there any new information in these FinCEN files that gives us new cause for suspicion or strengthens a cause that we previously decided not to file upon for some reason.

Just because one customer investigated or flagged on a transaction monitoring system was previously reviewed as not presenting any risk, if they now appear through the FinCEN files, the banking institution should reconsider that case.

The wealth of data we now have can be taken and run through the company to see if there is any exposure on the customer base. That's the number one priority.

Second, whenever something significant like this happens it's worth reassessing the financial crime risk assessment you did most recently. Reassess the systems and controls direction. This leak brings additional regulatory scrutiny, therefore if time was a little tight the last time you did your annual financial crime risk assessment, perhaps you were a little bit pressed to get the report to the board and you didn't answer or ask one key question, go back and ask them; go back and make sure you've got that financial crime risk assessment correct.

Just because the regulatory standards are at least once a year, it doesn't mean you have to do your assessment only once a year. You may wish to revisit it.

Go back to your systems and controls - maybe you've made a decision previously to exclude one or two key questions from the KYC process and maybe that's no longer justifiable. For example, do you only assess the customer's source of funds when you deem them to be high risk?

Can you determine if your customer is acting in line with the behaviour you expect? If they are transferring £300,000, is that typically what you'd expect? Perhaps not. Did you ask about occupation in the KYC process? Now is the time to revisit this.

CLOSING COMMENTS

Josh: The FinCEN leak remains a divisive issue. On one hand, the files shine a light on the scale of financial crime globally and present a reason for us to do better. On the other hand, we need to recognise it presents a significant breach contrary to the confidential nature of a SAR. These are documents that, by law, are confidential.

Significantly, the filing of a SAR does not mean the subject of the SAR is guilty of a crime. The SAR itself is simply that, it's suspicious activity report. The evidence remains the job of law enforcement and the courts. So if you see something in the leaks, don't immediately infer guilt, but use it to inform your risk assessment.

Article 11 of the UN's universal declaration of human rights states in a criminal trial the accused is afforded the legal right to presumption of innocence. In noncompliance speak, the accused is innocent until proven guilty beyond reasonable doubt. If you see somebody appear in the leaks, if I've talked about particular case, unless you've seen a declaration of guilt through the courts, it's an allegation alone.

LEAKING OF THE FINCEN FILES

ABOUT THE EDMUND GROUP

The Edmund Group was founded with the purpose of enriching the financial services marketplace for the betterment of customer experiences. They do this by collaborating with clients, all of whom are exceptional entrepreneurs or ambitious Fintechs.

The Edmund Group provides high-quality strategic advisory services rooted in a deep technical understanding of compliance, risk and financial crime disciplines honed with more than a decade of experience.

Their mission is to deliver compliance consultancy at a fair price that works for the individual needs of each client. They promise to always take time to get to know each client, whether they have a 1hour workshop or a 12 month retainer.

For more information, email jdeeks@theedmundgroup.co.uk

ABOUT PASSFORT

PassFort offers a single SaaS solution for full Customer Lifecycle Management. Headquartered in London, PassFort serves financial institutions of all types and sizes, processing more than 150,000 compliance journeys each month.

www.passfort.com | info@passfort.com