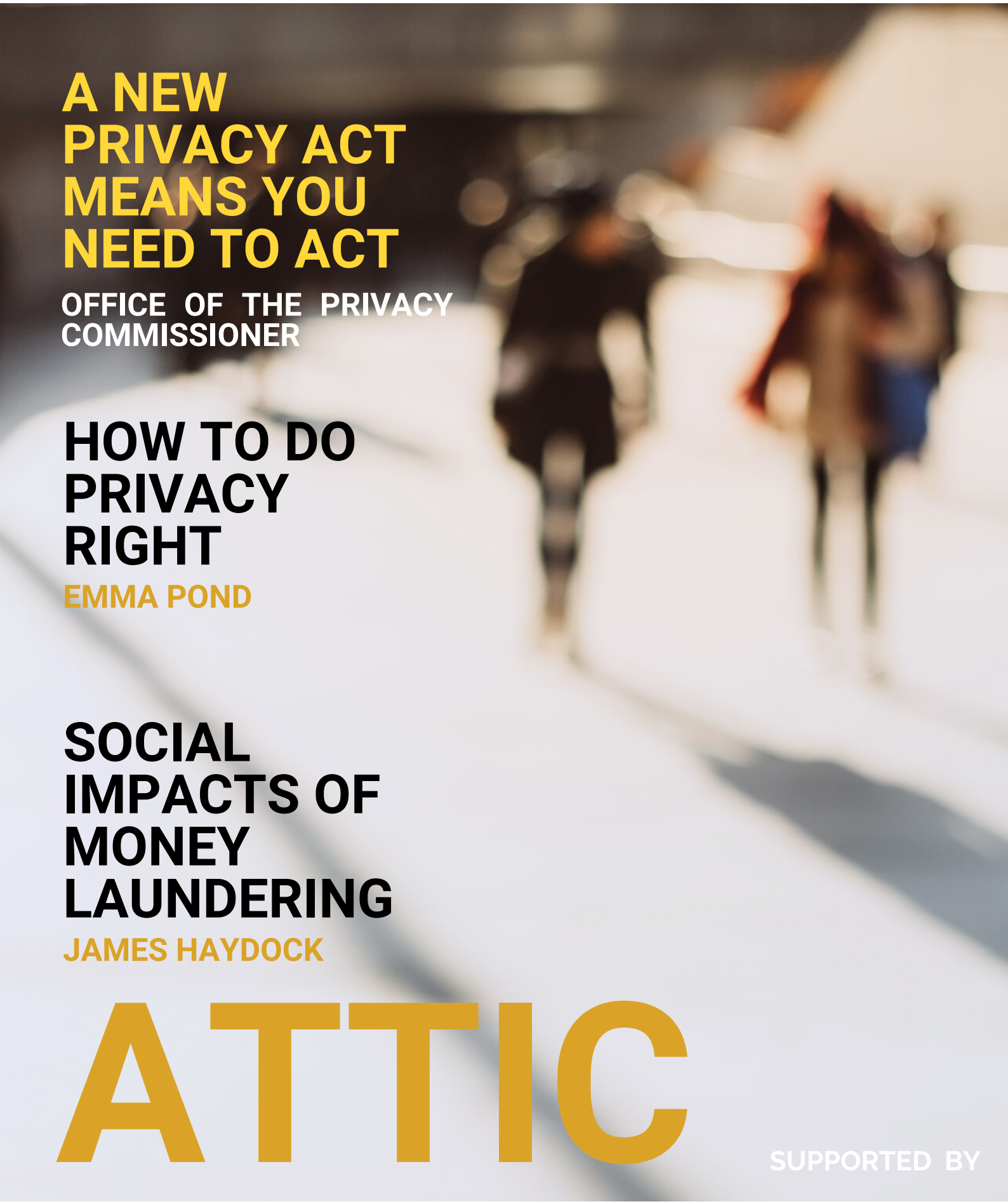
NOVEMBER 2020



A NEW PRIVACY ACT MEANS YOU NEED TO ACT

OFFICE OF THE PRIVACY COMMISSIONER

HOW TO DO PRIVACY RIGHT

EMMA POND

SOCIAL IMPACTS OF MONEY LAUNDERING

JAMES HAYDOCK

ATTIC

SUPPORTED BY

TIC co.

EDITOR'S NOTE

November has already been a 'month of weeks'. We have had Privacy Week, Fraud Awareness Week and the FIU/ACAMS Conference. Each a fantastic opportunity for us to learn more about the many nexus, nexuses, nexi, of anti-money laundering and to share our passion for all things AML/CFT with others.

It is great to see more media coverage of the extensive efforts undertaken by the FIU and Asset Recovery to put the intelligence you provide them via your reporting of suspicions into action. The growing amount of information, variations of sources and communication channels are providing lots of opportunities for the ATTIC Research Institute to continue its exploration into financial crime data both in New Zealand and overseas.

Members of our Auckland team have spent the week working from home as we focus on the safety and wellbeing of ourselves as well as our clients. It is safe to say that the shifting out of the office is now a relatively smooth operation. We have always supported flexible working arrangements. 2020 has definitely seen us up our game as we continue to explore new ways to use technology solutions to drive best practice, efficiency and job satisfaction.

Keep up the good work folks!

DR. ALICE TREGUNNA
Editor-in-Chief

ATTIC Research Institute
attic.nz

Partnerships and Support
info@attic.nz

Training
training@attic.nz

ATTIC RESEARCH INSTITUTE

A NEW PRIVACY ACT MEANS *YOU* NEED TO ACT

BY OFFICE OF THE PRIVACY COMMISSIONER

On 1 December 2020, New Zealand's updated Privacy Act comes into force. Here's what AML businesses need to know to prepare for the changes.

The world in 2020 is almost unrecognisable when compared to 1993 when the first Privacy Act was passed.

The Privacy Act 2020 significantly modernises New Zealand's privacy law and recognises the enormous technological advances of the past 27 years.

The new Act, like its predecessor, is based on information privacy principles that set broad standards around how organisations can collect, use, store and share people's personal information.

The updated Act gives the Privacy Commissioner additional powers including:

- The ability to issue compliance notices to compel organisations to do something – or stop doing something.
- The power to direct organisations to give individuals access to their personal information.

"There are new criminal offences for non-compliance and new fines. Some behaviour which has been optional will now become mandatory."

Privacy Commissioner
Te Mana Mātāpono Matatapu

Visit www.privacy.org.nz to access guidance and resources and to sign up for the Privacy Commissioner's fortnightly newsletter.

You can find additional information about the new Privacy Act in this blog.

To complete the "Privacy Act 2020" 30-minute online training module go to: elearning.privacy.org.nz.

CROSS-BORDER DISCLOSURE

New Zealand companies engaged in international trade need to get up to speed with the changes. The Privacy Act 2020 contains a new information privacy principle (IPP), principle 12, which sets rules around sending personal information to organisations or individuals outside of New Zealand.

Sending personal information overseas is known as "cross-border disclosure". Businesses and organisations are now responsible for ensuring that any personal information they disclose to organisations outside New Zealand is adequately protected. They must demonstrate that they have undertaken necessary due diligence before making a cross-border disclosure.

Personal information may only be disclosed to an offshore organisation if that organisation is:

- Subject to the Privacy Act because they do business in New Zealand.
- Subject to privacy laws that provide comparable safeguards to the Privacy
- Act – or they agree to protect the information in such a way (for example, by using 'model contract clauses').
- Covered by a binding scheme or is subject to the privacy laws of a country prescribed by the New Zealand Government.

If none of the above criteria apply, a business or organisation may only make a cross-border disclosure with the permission of the person concerned. That person must be informed that their information may not be given the same protection as provided by the New Zealand Privacy Act.

CLOUD STORAGE

A business or organisation may send information to an overseas organisation to hold or process on their behalf as their 'agent'. This will not be treated as a disclosure under the Privacy Act.

A typical example of this is an overseas company providing cloud-based services for a New Zealand organisation. The latter will be responsible for ensuring that their agent – the overseas company – handles the information in accordance with the New Zealand Privacy Act.

URGENT DISCLOSURES

A business or organisation may need to make a cross-border disclosure in certain urgent circumstances where it would not otherwise be allowed. IPP 12 allows cross-border disclosure when it is necessary to maintain public health or safety, to prevent a serious threat to someone's life or health, or for the maintenance of the law.

WHAT ELSE YOU NEED TO KNOW

If a business is issued with a compliance notice, it will have the opportunity to respond before it is finalised. Once finalised, the business can still appeal to the Human Rights Review Tribunal.

If the business loses its appeal and does not comply, or does not comply and does not appeal, it can be fined up to $10,000.

Because the new Act incorporates new criminal offences – with potential fines of up to $10,000 – businesses will now take on more financial risk when dealing with personal information.

The following behaviours are offences under the new Act:

- Failing to comply with a compliance order from the Privacy Commissioner.
- Misleading an agency to get someone else's personal information.
- Destroying someone's personal information when they ask for it.
- Failing to alert the Privacy Commissioner about a serious privacy breach.

USE THE NotifyUs TOOL

For businesses, one of the key changes to the Privacy Act is mandatory privacy breach notification. This means businesses must notify the Privacy Commissioner, and affected individuals, if there's a privacy breach that has caused serious harm – or could cause serious harm.
But how is "serious" defined? How does a business know if a privacy breach if serious enough to report?

The Office of the Privacy Commissioner has developed a new tool on its website called NotifyUs, that businesses can use to report privacy breaches. The NotifyUs tool assists businesses to assess whether their breaches are notifiable or not. Organisations or businesses that fail to notify privacy breaches can be fined up to $10,000.

HERE'S WHAT TO DO NOW

It's not too late to prepare for the changes to the Act. Here's what you can do today:

- Review the personal information your business holds and your information management practices. For example, could you provide someone with their personal information in a timely manner if requested?
- Develop a privacy breach response plan – who needs to be aware and involved?
- Consider any process changes you might need to make to incorporate the changes to the Privacy Act, such as mandatory breach notification. Assign someone in your business the role of privacy officer.


Privacy is precious
PROTECT IT. RESPECT IT.
Do you collect people's personal information?
The Privacy Act has changed.
Protect the personal information you hold.
Privacy Act 2020
Know what's new at privacy.org.nz/2020
Privacy Commissioner
Te Mana Mātāpono Matatapu

HOW TO DO PRIVACY RIGHT

BY EMMA POND

DIRECTOR - SIMPLY PRIVACY LIMITED

It's been a long time coming but finally, we have a new privacy law - the Privacy Act 2020, which comes into effect on 1 December 2020.
That's pretty soon, but don't stress too much if you haven't thought much about what its impact might be on your business – you still have time to get started.

At Simply Privacy we are all about supporting organisations (and their heroic Privacy Officers) to 'do privacy right'. And to help get you in shape for the new law we've made a checklist of the things we think every organisation that handles personal information should do before then.

The big changes are a new obligation to notify the Office of the Privacy Commissioner and affected individuals of serious privacy breaches; greater accountability when transferring personal information overseas (including a new Information Privacy Principle (IPP)); and new and stronger compliance and enforcement powers for the Office of the Privacy Commissioner.

As always, we suggest taking a risk-based approach, prioritising the actions that impact on the more sensitive and/or high volumes of personal information that your organisation handles. If you need more information, the Office of the Privacy Commissioner website has a lot to offer, and of course, if you need some help, we'd be happy to have a chat.

GET YOUR GOVERNANCE SETTINGS RIGHT

- **Appoint** a Privacy Officer, if you haven't already – it's a mandatory requirement
- **Formalise** your privacy accountabilities and reporting, to ensure that privacy gets the appropriate level of attention and resourcing for your organisation's risk level and risk appetite
- **Map** where personal information sits within your organisation's systems, and who has access to it

PREPARE FOR MANDATORY BREACH NOTIFICATION

- **Ensure** the systems holding your more sensitive personal information enable you to determine who has accessed what and when in the event of a breach
- **Check** your service providers have satisfactory security safeguards in place
- **Ensure** your service providers are required to notify you of a privacy breach and help you deal with it
- **Train** your staff so they can identify a privacy breach and know who to report it to
- **Establish** a privacy breach response plan
- **Practice** your privacy breach response plan with the right people involved
- **Draft** some notification communications to have ready to go (for the Privacy Commissioner and affected individuals)
- **Think** about who else you might have to notify in the event of a privacy breach (e.g. insurers/Police/under contract)
- **Ensure** you can manage a privacy breach in the midst of a privacy breach (e.g. if you can't access your systems)
- **Play** around with the online reporting tool 'NotifyUs' on the Office of the Privacy Commissioner website to get a feel for how it works

GET READY FOR CROSS-BORDER INFORMATION SHARING

- **Identify** what personal information your organisation is sharing overseas, and for what purpose
- **Remember** – disclosures to overseas service providers who are not using the information for their own purposes are not covered by the new IPP 12, but must comply with IPP 5 (your data must be kept protected)
- If you're sharing personal information with a 'foreign entity' that will use it for their own purposes, **ensure**:
  - An exception to IPP 12 applies to permit the disclosure (document your justification)
  - If you want to rely on the contractual exception, your current contracts provide for sufficient safeguards and limitations (The Office of the Privacy Commissioner has issued model contractual clauses that you can use, plus guidance)
  - Ongoing governance around cross-border information sharing, to ensure exceptions still apply (e.g. if relying on equivalent laws)

FINE-TUNE YOUR PROCESSES FOR HANDLING INFORMATION REQUESTS

- **Check** your identification verification processes to see if they are fit for purpose, including:
  - how to reduce the risk of impersonation
  - whether your staff understand and can identify when an information request may be made under threat of physical or mental harm
- **Ensure** your information request process allows requests for urgency to be appropriately considered
- **Check** your automated deletion processes can be paused to allow for the retention of personal information that has been requested under IPP 6

CONSIDER THE RELEVANCE OF TWEAKS TO OTHER INFORMATION PRIVACY PRINCIPLES

- **IPP1 – Purpose of collection - Review** what personal information your organisation is collecting, including personal identifiers, and make sure it's all necessary
- **IPP4 – Manner of collection - Check** if you collect personal information directly from children/young people and if so, assess whether this is being done fairly, transparently and proportionately
- **IPP13 – Unique Identifiers - Ensure** you're taking appropriate steps to minimise the harm of misuse of your unique identifiers

TAKE THE OPPORTUNITY IMPROVE GENERAL PRIVACY HYGIENE

- **Check** your external facing privacy statement is accurate and easy to understand
- Use the new law as a lever to get your people thinking about privacy not just as a compliance exercise but as an opportunity to build trust
- **Consider** whether you need to review your insurance coverage
- **Refresh** your information security awareness training for your staff – especially around email use and phishing, a significant cause of privacy breaches
- Don't forget your **employee** personal information – you have the same obligations there

EMMA POND: DIRECTOR - SIMPLY PRIVACY LIMITED

Simply Privacy is a specialist consultancy providing privacy advice, strategy and consultancy services to public and private sector organisations. They believe in a holistic, pragmatic approach to privacy practice and work with their clients to ensure that privacy solutions fit with their business needs and wider goals.

GOAML: WHAT IT IS & HOW TO USE IT

The goAML application is used by the Financial Intelligence Unit (FIU) to gather intelligence based on the suspicions of reporting entities to assist them in combatting money laundering and the financing of terrorism. Most do not realise that the system is not specific to the New Zealand FIU - and once you understand this some of the 'quirks' of the platform make a little more sense.

The goAML application was developed by the Organisation for Economic and Co-operation Development (OECD) as a strategic response to financial crime, in partnership with the UNODC Global Programme Against Money Laundering Proceeds of Crime and the Financing of terrorism (GPML). goAML has been specifically designed to meet the data collection, management, analytical, document management, workflow and statistical needs of any financial intelligence unit. Currently 56 of the 111 FIUs engaged with the OECD have deployed goAML.

Therefore, goAML acts as a central repository to establish a database of reports on suspicious financial activities and transactions across the spectrum of financial institutions and gate keeper reporting entities.

There are three primary solutions housed within the goAML sysytem to support members efforts to combat financial crime both in their own jurisdictions, across borders and internationally.

Collection: data is submitted by FIUs;

Analysis: rule-based analysis, risk-score, and profiling are performed byIU analysts;

Data Exchange: the exchange of data is:

a) between the FIU and the intelligence agencies or juridical authorities (within the framework of the national coordination) and b) between the FIU and regional institutions (eg. through FIU.net) and international ones (eg. Egmont Secure web).

Effective information sharing is one of the cornerstones of a well-functioning anti-money laundering and counter-terrorist financing (AML/CFT) framework. A key focus for the Financial Action Task Force (FATF) is to continue to develop best practices aimed at facilitating information sharing between the public and private sectors, and within the private sector, and its work on issues related to information sharing among public authorities—both domestically and internationally.

Key Benefits of goAML:

- designed as a modular system that fits the need of any FIU irrespective of size and is well suited to both low and high volume environments;
- an integrated system that can replace several disparate solutions;
- as a standardized product, it provides a comprehensive IT solution ata fraction of the cost of developing a one-off site-based solution;
- provides a standard and uniform Anti-Money Laundering platform to fight money laundering and terrorist financing;
- helps reduce the learning curve of new users with its standard graphical user interface.

Reporting entities should be familiar with goAML by now, as each has an obligation to have registered with the platform. It is far from a badge of honor to have not filed a suspicion to date with the FIU.

There are a few top tips below that can help you to use the system accurately, assisting both the team at the FIU and limiting the amount of filings you have rejected.

DEVIL IS IN THE DETAIL

Advice on getting the most our of your SAR and STR filings

Focus On Doing Your Part

goAML has undoubtedly frustrated a few reporting entities, but please remember that it is a tool used globally and therefore a few 'finickity' points do need to be worked through. But, as the media has shown us recently, there really is a point to filing your suspicions and continuing to support the New Zealand Police in their efforts counter money laundering and the funding of terrorism.

Forget the rhetoric of being a 'snitch'! It is important that we all look after our own industries and that we continue to reinforce the financial integrity of New Zealand's market place. You can report other individuals, companies and providers in your sector that are not 'playing by the rules' or where you believe they are not fulfiling their customer due diligence requirements.

goAML is YOUR goAML

Each reporting entity must be registered with goAML, so make sure that you know who has the admin rights for your organisation. The admin rights automatically sit with the first person who signed up for goAML. You cannot transfer your goAML user details to anyone else. For very good reasons these logins remain unique to a user, and reporting entities can and should have multiple users of the goAML platform.

To make any changes to your goAML accesses you are required to contact the FIU directly.

There are four different types of reports and terms in practice that should be used. These relate to either 'suspicions" (SAR/STR) or legislative prescribed transaction requirements (LCT/IFT). It is critical that you select the right one, due to the formatting within the goAML system, you cannot change reports part way through the filing.

In reality sometimes you may be required to file two reports, such as an LCT (large cash transactin) and a STR (suspicious transaction report). This is the same terminology that you should be using when you communicate with the FIU to prevent confusion.

So Many Bounce Backs? Know the difference between a SAR and STR

Get into the habit of saving pdf versions of the reports you file via goAML. They do not stay in the system for long. You are required to keep a register as well as suitable records to allow the activity or transaction to be recreated should further investigation be required. If you have a site visit from the FIU, your sector supervisor or another investigatory body you will be expected to be able to produce these.

TIPS TO HELP YOURSELF AND THE FIU

Your SAR/STRs are all reviewed by a human at the FIU in Wellington and so it is important to get it right to prevent unnecessary delays. Make sure that you are concise and do not use industry specific jargon.

- Suspicious activity reports **always** have a monetary amount of $0 and are **always** a multi-party transaction.
- There are three party type options (person, account and entity) **but** the 'entity' option is used very infrequently and it is unlikely you will need to select it.
- To determine if someone is 'your client' or 'not your client' review whether you have done customer due diligence on them at the time of onboarding.
- Account number does not mean bank account nuimber. The FIU wants to know the unique identifier you have for the person who has caused your suspicion.
- Your institution code is the goAML code that was given to you when you registered.
- If you have both the persons passport and their driver licence **always** use the passport details to provide their full legal name.
- **Always** use NZD when documenting monetary amounts in your reports.
- You have 10 days to file your LCTs from the date of the transaction and it can be easier to work through them in batches every week or two if you have lots of them.
- If you have the IP address for where the momey has come from in a transaction then provide this to the FIU.
- When asked when the relationship or situation was 'opened' this is referring to the date when you initially onboarded the client.

New Zealand's financial intelligence unit is one of only five in the world that is housed at Police Head Quarters - giving them access to police databases as well as allowing them to act quickly on the intelligence provided by reporting entities and the public.

5 MINUTES WITH AN EXPERT: ADAM HUNT

FFOUNDER AND DIRECTOR AT THE TRUST, INTEGRITY AND COMPLIANCE COMPANY (TIC CO.)

AN INTERVIEW WITH ADAM HUNT
BY NAT STAGG

Please tell us a bit about your background, describe your current role and your responsibilities.

I have a bit of a short attention span which has lead to a career in varied industries. Initially, I started out in the IT industry as an engineer and architect and eventually CIO. I shifted into regulatory compliance at the NZ Inland Revenue Department where I implemented an intelligence led philosophy in the compliance function. After some time working in a global role with Oracle Corporation, I joined the NZ Financial Markets Authority to establish its strategic intelligence function.

Since leaving FMA, I founded The TIC Company, whose board I continue to chair.

What is your opinion of the current AML/CFT regime within New Zealand? And, how does this compare internationally?

We've had our AML/CFT regime in place since 2013. We phased the rollout, and we put multiple agencies in place to tackle different market segments.

This has lead to regulatory gaps, delayed guidance (as multiple regulators have to agree everything), and from a customer perspective, different experiences depending on what type of entity you are dealing with which causes frustration and reduces confidence in the regime. I think it would be wise to transition to a single AML/CFT supervisor for New Zealand, establishing a single point of truth and approach to allow the focus necessary to tackle international financial crime.

What made you interested in AML/CFT and financial crime?

I'm all about the regulatory craft, with my core interest being - how do we get effective outcomes that minimise harm in our global community without undue burden to the entities tasked with enacting the regime.

What is the most important thing you have learned when it comes to AML/CFT?

You've got to get buy in from your team, from your front line staff right through to your senior managers in order to run an effective, compliant programme in your business.

What would you consider to be a key thing people forget or do not understand when it comes to AML/CFT?

The consequences of inadvertently facilitating ML or TF would be reputationally devastating, probably an existential threat to a firm whose clients are very likely to go elsewhere.

When confronted with the drudgery of yet another thing to comply with and evermore boxes to tick before getting to business, people quite naturally forget why we are doing this.

Predicate offences and the flow on harms inflict on communities for example the trafficking drugs, I think most of us can agree are worth the effort to assist in reducing.

How do you tend to keep up to date with all things AML/CFT?

Oh, I am on the mailing list for about every industry related update, newsletter or blog.

What is one of the most rewarding parts of working within your sector and supporting the AML/CFT regime within New Zealand?

One of the most rewarding parts of creating an AML Outsource provider is offering reporting entities a cost effective, compliant solution that allows them to do the right thing from an AML perspective, while freeing up time to get back to their core focus.

ADAM'S TOP TIPS

- GET THE BASICS RIGHT: IDV, REPORTING, RECORDING KEEPING, RED FLAGS, KNOW YOUR CUSTOMER.
- DON'T FORGET THAT YOU'RE PART OF A CHAIN: SOMEONE ELSE WILL ALSO BE CONDUCTING DD AND THEY MAY BE BETTER OR WORSE THAN YOU. FORM YOUR OWN OPNION.
- REFLECT: WRITE DOWN WHY YOU MADE THE RISK DECISION? WHAT PRESSURE DID YOU FEEL FROM OTHER STAFF OR REPORTING ENTITIES?

SOCIAL IMPACTS OF MONEY LAUNDERING

Without crime there is no money laundering or victimisation.

SOCIAL DISINTEGRATION

Organized crime perpetuates and exploits individuals and communities.

HUMAN TRAFFICKING

Organized crime profits heavily from the forcible relocation of people, using them as commodities.

CORRUPTION

Corruption strengthens the link between organized crime, politics, and society, impacting the very fabric of democracy and highlighting systemic inefficiencies.

DRUG DEALING

“There are only two industries which refer to their customers as users, one is technology, and the other is the illegal drugs trade.”

ECONOMIC MONOPOLY

Money laundering 'front' businesses jeopardize the stability of the legitimate market and can squeeze legitimate businesses out of the market.

THE SOCIAL IMPACTS OF MONEY LAUNDERING

BY JAMES HAYDOCK

BACHELOR OF ARTS (CRIMINOLOGY) STUDENT & ATTIC RESEARCH INSTITUTE INTERN

Without crime there would be no illicit funds generated to launder. The same relationship dynamic often occurs between victims and crime; to acquire the funds to launder in the first place, victimisation is often an implicit social consequence of criminal activity. Hence, the impact link between money laundering (ML) and society. The following analysis aims to explore ML's link to organized crime, and the subsequent social effects both incur.

Money laundering is assumed to happen purely through financial institutions (Lilley, 2003). While this is usually needed to clean the funds for legitimate use, the bartering and trading of goods and services is a frequent (if not more popular) avenue utilized to generate and clean the illicit funds (Lilley, 2003).

Trading has two different outcomes: firstly, the trading of goods to generate the illicit funds in the first place, which is a primary offence, with the social impact often including some form of human victimisation due to crime facilitating the generation of money; secondly, the trading of goods to clean money which then enters the funds into the legitimate system, evoking socio-economic and, the potential for, political implications (Unger & Busuioc, 2007; Fabre, 2003). This is all advantageous for criminal organizations as it provides opportunity for exploitation of low risk/high profit criminal endeavours (Fabre, 2003; Herrera, 2009).

Fabre (2003) states organized crime is the most effective and consistent way to generate and maintain the flow of illicit funds. Fabre (2003) continues that this is because within any organized crime that is committed, they exert coercive power over a population or territory with the sole objective of legitimately monetizing the proceeds of often multiple criminal activities, and eliminating the competition (both illegal and legal rivals ie. legitimate businesses or alternate crime syndicates). The trading of goods and services is then crucial towards the effective functioning of organized crime (much like a legal business) (UNODC, 2018). This has social effects, partly due to the victimisations it incurs, and partly due to the money that is subsequently laundered.

I will outline these main social impacts below.

SOCIO-CULTURAL DISINTEGRATION

Socio-cultural disintegration is a phenomenon in which low-employment rates, an absence of government attention, unwarranted subsidising of the economy, and cultural animosity all create strain on the population, for which people turn to illegitimate means to alleviate said strain (Fabre, 2003; Agnew, 2001). Organized crime will play on this to recruit labour and exploit hardship, which elicits an obvious social impact as the strain facilitates the creation of an illicit labour force - essentially organized crime (Fabre, 2003).

This also has the opposite effect by breaking down members' ties to formal society, essentially perpetuating the continual disintegration of that individual's social and cultural norms and values. Victimisation then occurs both ways: on the victims of the crimes; and the subsequent disintegration of (new) criminals previous norms by persistent interaction with a criminal environment, and the generation of illicit proceeds which lessens the strain.

HUMAN TRAFFICKING

Evidence sets are proving that criminals are trafficking humans at an increasing rate as it is deemed to be a profitable venture (FATF, 2011). This has a major social impact, primarily on the victims of trafficking as not only have they been taken from comfort, but often implicit in this crime is subsequent integration into the illegal trade market, with sex trade identified as a profitable endevour for crime syndicates (Lilley, 2003). Many victims are also provided goods by their offenders, which is then used to blackmail and maintain the power dynamic (another goods/service transaction) (Herrera, 2009). Organized crime is the most likely source of human trafficking as the proceeds generated from this are extensive (between 32 and 34 billion US dollars per-annum from approximately 2.45 million persons exploited per year (FATF, 2011; Herrera, 2009)), almost all of which will need to be laundered into the legitimate system for future use. This then provides the resources to continue trafficking the trading of goods and services (in this case humans are the commodity) which has become so profitable for organized crime (Herrera, 2009; FATF, 2011). Victimisation is then the clearest, and most destructive, social effect here as human trafficking is facilitating the uprooting and separation of families and communities.

CORRUPTION

Corruption regarding money laundering is first and foremost a systematic occurrence as throughout the money laundering process the first step, referred to as ‘placement’ (which denotes the placing of laundered money into the legitimate system), is the most vulnerable stage for identification (Unger & Busuioc, 2007). Therefore, instances occur where the system is corrupted through third party failures (Unger & Busuioc, 2007), such as accountants or lawyers purposely failing their due diligence obligations. The social impact of this then is the diminishing legitimacy of the government, especially if knowingly involved, as they are supposed to uphold the intrinsic values of their society (Fabre, 2003). It also has social implications on the market, as large countries can process a higher quantity of transactions, which allows for exploitation of loopholes detrimental to businesses, consumers, and the market more frequently than before (Lilley, 2003). Therefore, corruption strengthens the link between organized crime, politics, and society, impacting the very fabric of democracy and highlighting systemic inefficiencies.

DRUG DEALING

"There are only two industries which refer to their customers as users, one is technology, and the other is the illegal drugs trade" (Baxendale, 2019). The meaning behind this quote - that human attention is the commodity being sought to exploit - is the exact business model that organized crime employs (UNODC, 2016). The selling of drugs, which is a consistently profitable business, subsequently has a huge impact on society given it perpetuates increased drug use. The United Nations Office on Drugs and Crime (UNODC) (2005) estimated the illicit drug trade is worth a retail value of $321 billion US dollars, which they state interferes with almost all levels of human security, such as health, and social and economic well-being (both state and individual). Not only do drugs compromise the fabric of society, but also the integrity of financial institutions. Fabre (2003) estimates that the money elicited annually through drug trafficking could generate, in a single decade, seven times its original worth in interest - providing more incentive for aforementioned institutional and/or political corruption. Given the Ministry of Health (2016) estimates the social costs and intervention costs of drug related harms is $1.8 billion NZ dollars, there is a clear social impact link between organized crime (who traffic and supply) and the victimisation of their 'users'.

ECONOMIC MONOPOLY

Unger and Busuioc (2007) state that calculating effects of ML is a struggle given the subjective challenges each country incurs, and criminals will create and exploit institutional loopholes relative to noticed risks. What this does is compromise the integrity of financial institutions and markets, such as emerging markets in countries integrating into the international financial system as this poses new subjective risks (McDowell, 2001). McDowell (2001) continues, explaining the undermining of legitimate private sectors is one of the "most serious microeconomic effects of ML" (p.7) as the ability to provide goods and services through 'fronts' (cash based businesses created to launder money discreetly) and subsidised prices, jeopardizes the stability of the legitimate market, which leads to the undermining of the markets and loss of financial policy control. Legitimate businesses are then squeezed out of markets (Lilley, 2003), which transfers economic monopoly to the crime syndicates, affecting the way, and what in fact, society consumes, essentially corrupting the basis of macroeconomics (McDowell, 2001). As ML generates between 2 and 5% of the world's gross domestic product (McDowell, 2001), the impact ggrrelationship between organized crime, ML, and society is clear as it affects the way in which consumers consume goods and services, therefore, dictating the direction of the economy.

To conclude, Rueter (2005) explains that preventative money laundering mechanisms are not solely there to stem the flow of laundered money. While this is still a clear aim, the overarching goal of AML/CFT is to reduce the frequency of illicit activities which ensure growth within organized crime (Rueter, 2005). The aforementioned social effects are not then subjective to one country. The effects are a global combating challenge as laundered money (and implicitly the original crimes) flows through the majority of financial institutions worldwide (FATF, n.a). Effects such as social-disintegration, corruption, economic monopoly, and the trafficking of humans and drugs especially, therefore evoke clear victimisation, and the root cause is the activities perpetrated by organized crime syndicates to either generate their illicit funds, or to clean such funds. As a result, the possible social and political effects of money laundering, if left unfiltered, are serious (FATF, n.a), not just for the economy, but the people and fabric of society and democracy.

FRAUD AWARENESS

THE FRAUD AND ANTI-MONEY LAUNDERING NEXUS

Fraud is Predicate Crime for Money Laundering

Fraud is the intentional manipulation of the truth for financial or personal gain. It can be a person or a 'thing' that intends to deceive others, typically by unjustifiably claiming or being credited with accomplishments or qualities.

Fraud perpetrators target businesses, governments and individuals.

69% male

40% 35-45 years old

50% 5 years or more with company

53% act alone in the scheme

50% have a university degree

46% live beyond their means

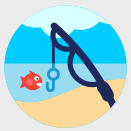
88% never been charged or convicted

REMEMBER: Where there is fraud there is money laundering.

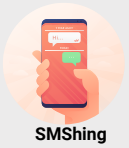
Common Techniques of Fraudsters

Taking physical information, relying on social engineering or data breaches.

Tech is great and implementing smart solutions to support your AML compliance has been essential. BUT tech solutions can be exploited for fraudsters gain if they are not implemented and managed correctly.



Phishing
email manipulation to provide sensitive data which is then exploited



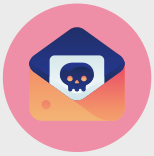
SMShing
using text messages to lure victims instead of an email or phone call

Pharming
controlling a legitimate domain and redirecting traffic

Worms
self replicate and spread

Keyloggers
track what is typed

Spyware
collecting data about computer user



Ransomware
lock out and demand payment for access

REMEMBER: Protect yourself, be curious and always ask questions.

Internal Control Weaknesses Contribute to Fraud

Smaller organisations are more likely to lack the internal controls, however, larger ones are more likely to have their internal controls overridden.

Code of Conduct: Make sure that your expectations for AML compliance are clear, documented and your team are fully trained.

Internal Audits: Regularly check that the systems you have in place are fit for purpose. Do not rely only on your external audit.

Regular Management Reviews: A 'poor tone at the top' prevents the smooth running of an anti-fraud and anti-money laundering regime. Management must enforce a culture of compliance and support the compliance officer.

Be careful to avoid creating or re-enforcing a culture of 'exceptions'. It is important to have documented exceptions procedures and registers BUT overriding of your AML controls on a regular basis increases both your risk and your clients risk of becoming victims of fraud. Also, be mindful and commit to your ongoing customer due diligence requirements. This protects your businesses as well as your clients from idenity theft and fraud.

REMEMBER: Stay alert, monitor and report any suspicions.

Effective Record Keeping and Reporting Mechanisms

The historical division between AML and anti-fraud has evolved into a cultural and mindset split creating disconnects and data silos.

AML know-your-customer procedures and documentation of customer's expected activity can serve as an important fraud tool.

The breaking down of silos within your otganisation can lead to better identification of fraud and money laundering schemes that cross channels, products, and lines of business. This will also allow for greater visibility for management through aggregated data reporting, providing a more holistic business-wide view.

You don't have to be a reporting entity to file a suspicion with the FIU.

You can also get in touch via goAML@police.govt.nz

BUT - if you think that a criminal offence has taken place then you should report it to your local police station or online at 105.police.govt.nz

Want to know more?
Contact me: draml@ticc.nz

UPDATES

AML/CFT TRAINING

WEBINARS

If you are looking for expert guidance around your AML/CFT obligations, sign up for ATTIC's regular instructor-led webinars.

Book in for your training today! We run a range of fixed training sessions every week across a range of topics. These 1 - 1.5 hour sessions cover AML topics in-depth and are open to everyone.

We also have more specific and advanced courses available to our clients. Get to touch today to see how we can tailor your training session, specific to your needs.

Thank you to those who have booked and recently attended their training sessions!

LEARN MORE

PROFESSIONAL COURSES

The recent 2020 DIA Regulatory Report found that insufficient training of compliance officers, senior management and any staff member with AML/CFT duties was one of the most common areas of non-compliance.AML/CFT training should be taken seriously, and it should be provided consistently. We have a number of courses below to suit both individuals and businesses to complete training requirements.

We provide these courses Online, In-Person and One-On-One. We also offer pre-recorded training packages. Please fill in our form below to find out more.

SUBMIT AN EOI TODAY!

ATTIC RESEARCH INSTITUTE

UPCOMING

EVENTS & OPPORTUNITIES

AUCKLAND KNOWLEDGE NET: PRIVACY ACT 2020

Thursday, 3rd December 2020

Simpson Grierson is hosting the next Auckland KnowledgeNet meeting for The International Association of Privacy Professionals at its Auckland office.

Hear from Privacy Commissioner John Edwards on what the new Privacy Act will mean for businesses and organisations in practice, how the Office of the Privacy Commissioner will be implementing the reforms, the new approach to enforcement and compliance and key areas of focus for the Office over the next 12 months. The event will be followed by networking drinks.

To learn more and register, click here.

PRIVACY AND DIGITAL IDENTITY WEBINAR

As the Privacy Act is coming into force on 1st December this year, tune in to hear experts in this talk on the Privacy Act and the importance of good privacy practice: Liz MacPherson (Assistant Privacy Commissioner), Karen Ngan (Partner at Simpson Grierson) and our very own Alice Tregunna (CEO of TIC Co.).

The Privacy and Digital Identity webinar is now available online, you can access the full session here.

WRAP UP 2020 WITH THESE DIGITAL IDENTITY NZ WORKSHOPS!

The below workshops are for DINZ members only. Not a DINZ member? Join here.

AML Reliance Workshops

Register for one or both of the below workshops. These will be collaborative meetings to address questions, challenges and opportunities arising from the DINZ AML Reliance report.

Dates: 30 November 2020 & 14 December 2020
Time: 11:00am - 12:00pm
Location: Online
Cost: Free

To learn more and register, click here.

Trust and Identity Workshop

This next DINZ member session further discusses the education gap that was found in the DINZ 2020 Trust and Identity research, and start work on shaping educational materials to fill that gap.

Dates: 21 December 2020
Time: 11:00am - 12:00pm
Location: Online
Cost: Free

To learn more and register, click here.

INDUSTRY UPDATES

OPERATION BROOKINGS

Police arrested six people and seized millions in assets after early morning raids in Auckland last month.

Seven high-end luxury vehicles, a boat and three motorbikes - with a combined value of more than $1.2 million - were seized by police alongside three properties, worth at least $3.3m, and about $250,000 in cash.

READ MORE

FIU / ACAMS CONFERENCE

This year's FIU (NZ Police) / ACAMS AML/CFT Conference ran from 9 - 11 November in Wellington. Themed as "Organised Crime - Money Feeds the Beast", the Conference focused on how money is the key motivator for a range of criminal offending.

READ MORE

PRIVACY WEEK

To celebrate Privacy Week, the Office of the Privacy Commissioner, New Zealand has launched a new campaign to highlight the importance of protecting and respecting personal privacy alongside the new Privacy Act 2020.

If you collect personal information, learn what your obligations are and obtain resources and read more here.

READ MORE

109KG OF METH SEIZED

A man was sentenced to 14 years and seven months' imprisonment for his role in trying to smuggle more than 109kgs of methamphetamine into New Zealand.
The seizure by NZ Customs prevented up to $135 million dollars of potential social harm to our communities.

READ MORE

OPERATION SKIPJACK

NZ Police successfully seized over $5 million in controlled drugs last week - causing a certain significant disruption in the illicit drug market.

READ MORE

OPERATION MARTINEZ

NZ Police carried out 23 search warrants across Auckland following an investigation by the Financial Crime Group into money laundering and related offending.

Nine individuals are facing money laundering and related charges and appeared in the Auckland District Court, with one of them also facing charges relating to the methamphetamine supply.

READ MORE

FRAUD AWARENESS WEEK 2020

15 - 21 NOVEMBER

Fraud Awareness Week is a cross-government initiative aimed at getting people to talk about scams.

Scam and fraud reports to Netsafe rose by 73% in the April – June 2020 period which covered the majority of the COVID-19 lockdown.

NZ Police's Financial Intelligence Unit estimates New Zealanders lose $20-30 million annually to scams. In the United States, the estimated annual losses are $US650 million.

Anyone can get targeted by scammers.
Here are some resources to help you and your organisation stay safe:

- The Ministry of Business, Innovation and Development and Consumer Protection are raising awareness of the common signs of scams and tips to stay safe.
- Consumer Protection NZ share tips on how to identify a scam, how to avoid them, and where you can get help.
- Think you know your stuff? Visit the International Fraud Awareness Week website to test your knowledge and access various guides and reports to become an expert.

WOMEN IN AML NETWORKING SESSIONS

AML/CFT has attracted a large amount of hugely successful women to the field. The Women in AML Networking Sessions are an opportunity for everyone to get together, share knowledge and support each other in the sector.

On behalf of the **TIC Company & ATTIC Research Institute** and **ACAMS** we would like to thank everyone who joined us at our first Women in Compliance/AML Networking event.

The Network will be running a range of sessions next year, including; networking events, seminars, workshops and so much more. We look forward to seeing everyone again at our next event in 2021! Keep an eye out for more information coming soon.

To express your interest in joining the Women in AML Network, get in touch with us at: ***info@ticc.nz.***

TIC CO. ACAMS

Find us on Facebook

ATTIC RESEARCH INSTITUTE