GARY HUGHES
BARRISTER

M: (+64) 021 477 780
T: (+64) 09 558 5877
E: gary@garyhughes.nz

PO Box 178
Shortland Street
Auckland 1140

PRIVACY AND CYBER LAW (Regulatory, Recovery and Reform)

Legal tools and tips – for ANZIIF CYBER RISK MANAGEMENT

Gary Hughes, Akarana Chambers, Auckland
August 2018

PRIVACY-CYBERCRIME-BLOCKCHAIN-RANSOMWARE-CRYPTO: what to COVER?

(a) Big picture themes − anonymity, hacking, leaks, fraud

(b) Regulatory approaches − a work in progress

(c) The Privacy Bill − legal overhaul for NZ

(d) Mandatory data breach notification − Aust comparisons

(e) GDPR and international overlapping regimes

Phew! − pause − watch − pivot

(a) The fraud problem, digitally magnified across borders

(b) Recalibrating: good and bad responses to an e-fraud

(c) Engage with law enforcement? Or use civil asset recovery

(d) Bitcoin + Blockchain + Bad Guys: follow the virtual money?

GARY HUGHES
BARRISTER

BIG DATA / BIG HOLES / BIG PUBLICITY

Data leaks probably the “new normal” – nobody impregnable

Cyber crime for commercial/national/political advantage – Trump Analytica

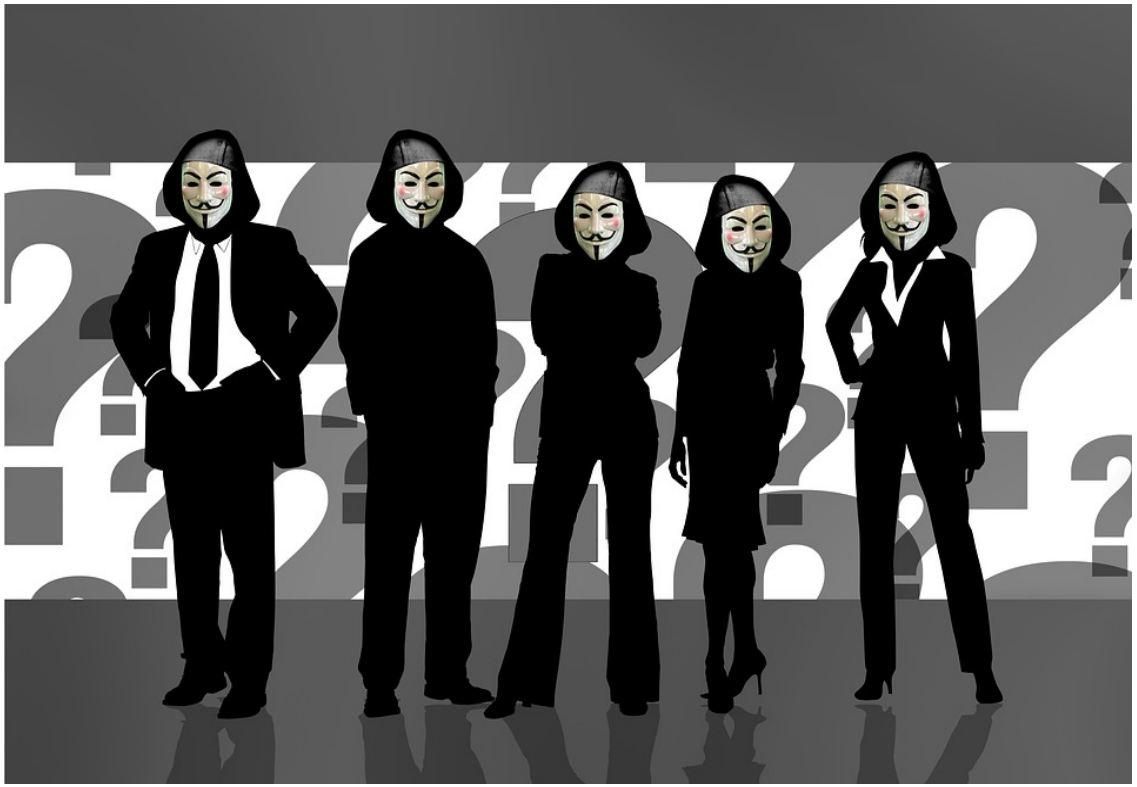
Privacy laws and supervisory regimes, toughened in response – duty to customers, duty to dob yourself in (but when and how, how publicly?)

- Court of public opinion (twitterati) more important than court of law
- Brand destruction - if you have to tell the market, how to manage that?

GARY HUGHES
BARRISTER

BIOMETRICS VS ANONYMITY

- Conundrum – we have more data, personalised offers, less personal contact
- Uber or hail a taxi; online account or a bank teller; crypto or cash



- Email abuse (CEO business compromise fraud)
- 2 factor security not enough
- Voice recognition
- Facial recognition, biometrics and fingerprinting
- Blockchain immutable and digital ledgers permanent
- Who is behind it?

Who shares? controls? profits?

ENFORCING 'CONDUCT'

FMA Conduct Guide 2017 – Royal Commission 2018

Conduct is a lens through which to see other activity? (whose lens?)

Questions to ask at all levels - especially governance level

Put the client interests at the core (i.e. moderate your own base instinct for profit?) and don't opt the customer in by default

Internal codes of conduct – internal enforcement? Whistleblowing?

What level of tolerance for poor behaviour? Cavalier cyber practices?

UK's response to the Panama Papers – criminal offence of failure to prevent criminal conduct (tax evasion) and now beneficial ownership registers

GARY HUGHES
BARRISTER

OBFUSCATION & MIS-SELLING & INSECURE

Misrepresentation, misleading, deceptive, or non-disclosure of

- Or overdisclosure?
- Sales, tracking, sharing abuse
- Bundled or opaque policies and products
- Pressure selling of terms
- Fine print too fine, complex and increasingly hard to read
- Financial products not suitable, not fit for purpose or for customer
- Hushing it up when you leak

OFFICE OF THE PRIVACY COMMISSION

IN THE PAST:

- Privacy Act 1993 languishing, seen to lack bite, no real sanctions
- But a huge overseas focus (Edward Snowden, Facebook, EU GDPR); local issues too (GCSB surveillance, marketing databases, ransom-malware)

But these days:

- John Edwards a more active Commissioner, began using power to name and shame, doubled budget funding of the Office, pressing for law reform
- Tackling Veda for misuse of credit check database
- Cyber security risk now has a voice at the top level Board-table

PROPOSED OVERHAUL:

- Mandatory reporting of data breach (loss, leak, hack); New offences with $10,000 fine – eg. fail to report breach; to destroy documents if person has sought access to data

The proposed Privacy Act overhaul

Privacy Bill will repeal and replace the existing Privacy Act 1993, as recommended by the Law Commission's 2011 review of the Act.

The Act has been in operation now for 25 years. Pre-Internet is Pre-historic. Much has changed in that time; the law is always running after technology.

How personal information is collected and used has drastically changed with the rise of the internet and the digital economy, social media platforms, e-commerce, algorithms, tracking, AI, and cloud storage.

Large amounts of data can be readily stored, retrieved and disclosed or sent around the world. While there are efficiencies and many consumer benefits for the positive, it does create new challenges for protection of personal information. So the legal pendulum might swing hard the other way.

The 12 IPPs remain - Privacy Act basics

Bill has retained the Act's existing 12 information privacy principles:

1. Purpose of collection of personal information
2. Source of personal information
3. Collection of information
4. Manner of collection of personal information
5. Storage and security of personal information
6. Access to personal information
7. Correction of personal information
8. Accuracy of personal information to be checked before use
9. Personal information not to be kept for longer than necessary
10. Limits on use of personal information
11. Limits on disclosure of personal information
12. Unique identifiers

The principles have been updated in some respects, for example, to better protect personal information that is being shared/sent overseas.

GARY HUGHES
BARRISTER

The 12 IPPS summarised in simple terms

1. Only collect personal information if you really need it
2. Get it straight from the people concerned where possible
3. Tell them what you're going to do with it
4. Collect it legally and fairly
5. Take care of it once you've got it
6. People can see their personal information if they want to
7. They can correct it if it's wrong
8. Make sure personal information is correct before you use it
9. Get rid of it when you're done with it
10. Use it for the purpose you got it
11. Only disclose it if you have a good reason
12. Only assign unique identifiers where permitted

PRIVACY COMMISSION VIEW:

Together, these principles form a 'life-cycle' for personal information.

Agencies must:

- **decide what information they need**, and where and how they are going to get it
- ensure they **hold the information with appropriate protections**
- comply with any **access or correction** requests they receive
- keep information secure, **use and disclose with care**, and in line with the purposes

The proposed Privacy Act overhaul

Privacy Bill reform timeline:
Introduced to Parliament, 20 March 2018
First Reading, 11 April 2018
Submissions deadline, 24 May 2018
165 Submissions were made
Select Committee (Justice Committee) report due 22 November 2018

Proposed enactment 6 months before commencement – so 1 January 2019
Proposed commencement date 1 July 2019
Transitional provisions are contained in schedule 1.

There is no summary of submissions available yet − hopefully Ministry will release something. But all the individual submissions are available online.

The PC is still keeping up the political drive for reform

Main changes – substance of Privacy Bill

Mandatory reporting of privacy breaches: privacy breaches (unauthorised or accidental access to, or disclosure of, personal information) that pose a risk of harm to people must be notified to the Privacy Commissioner and to affected individuals:

Compliance notices: the Commissioner will be able to issue compliance notices that require an agency to do something, or stop doing something, in order to comply with privacy law. The Human Rights Review Tribunal will be able to enforce compliance notices and hear appeals:

Stronger cross-border data flow protections: New Zealand agencies will be required to take reasonable steps to ensure that personal information disclosed overseas will be subject to acceptable privacy standards. The Bill also clarifies the application of our law when a New Zealand agency engages an overseas service provider:

New criminal offences: it will be an offence to mislead an agency in a way that affects someone else's information and to knowingly destroy documents containing personal information where a request has been made for it. The penalty is a fine not exceeding $10,000:

OPC can make binding decisions on access requests: this reform will enable the Commissioner to make decisions on complaints relating to access to information, rather than the Human Rights Review Tribunal. The Commissioner's decisions will be able to be appealed to the Tribunal:

OPC gains stronger information gathering powers: the Commissioner's existing investigation power is strengthened by allowing him or her to shorten the time frame within which an agency must comply, and increasing the penalty for non-compliance.

Mandatory reporting of data breaches

Must notify the OPC "as soon as practicable"

- "**privacy breach**":
  - unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, the personal information; or
  - an action that prevents the agency from accessing the information on either a temporary or permanent basis

"**Notifiable privacy breach**" – one that has caused any of certain listed types of harm

"**affected individual**" includes: the individual to whom the information (breach)relates; whether inside or outside New Zealand, and even a deceased person

ENFORCEMENT TOOLS: OPTIONS MOST AGENCIES HAVE

A flexible range of tools/responses to a breach:

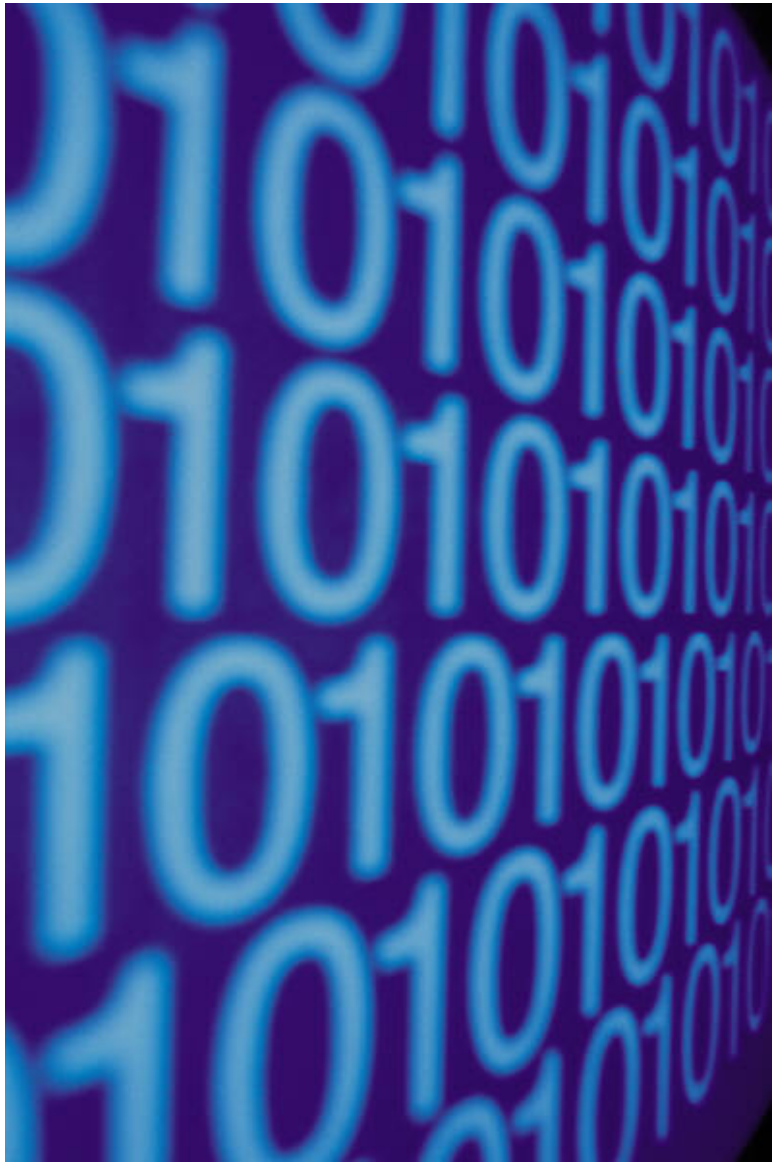
- Issue a formal warning (private or public)
- Accept a written, court-enforceable undertaking
  - breach of undertaking terms can lead to orders to pay amount of any financial gain, or % of turnover, compensation claims in HRRT
- Seek Court injunction: performance/mandatory, or restraining
- Civil proceedings seeking penalty, on balance of probability
- Criminal prosecution seeking fine/imprisonment, on standard of 'beyond reasonable doubt'
- Reputational Risk - PR and media usage by enforcers and defendants

Over time, likely to develop other mechanisms – adapt overseas concepts, new codes/guidelines or elevated notions of 'best practice'

GARY HUGHES
BARRISTER

PHEW!
PART TWO

- E-Fraud Responses
- and Recovery



The Fraud Problem in the modern era

Fraud and corruption cases are pervasive, complicated and often cross national boundaries.

Redress and recovery is hard; local courts of little use.

Money moves faster than victims can (at least, without sophisticated assistance) – digital era has made it worse

Victims do not know what to do, or who to turn to for help.

Law enforcement has scarce resources, and:

- a different focus, on apprehension of fraudsters and imposing criminal sanctions
- few helpful initiatives or real asset recovery avenue for victim

GARY HUGHES
BARRISTER

Cyber fraud - problem magnified by technology

- Who do you trust on the internet?
- Anonymity/encryption − sought out by the rogues
- So rapid, it's instant. How quick can you respond? Are you part of the problem?
- How can you find an owner, or an asset, IT records, even an authority in charge of the foreign email provider or cryptocurrency?
- Where do you sue? (local victim or rogue's destination)

Cyber problems magnified across borders

- Inbound and Outbound investment/immigration
- Who do you trust to locate, investigate, sue or recover the asset in that far-flung destination?
- Ownership of assets vs registration of assets
- NZ/Aust as a fraud (or ML or corruption) destination, or a fraud exporter/producer jurisdiction
- Countries each set their own (inconsistent) laws, but crypto-assets and cyber-crims don't

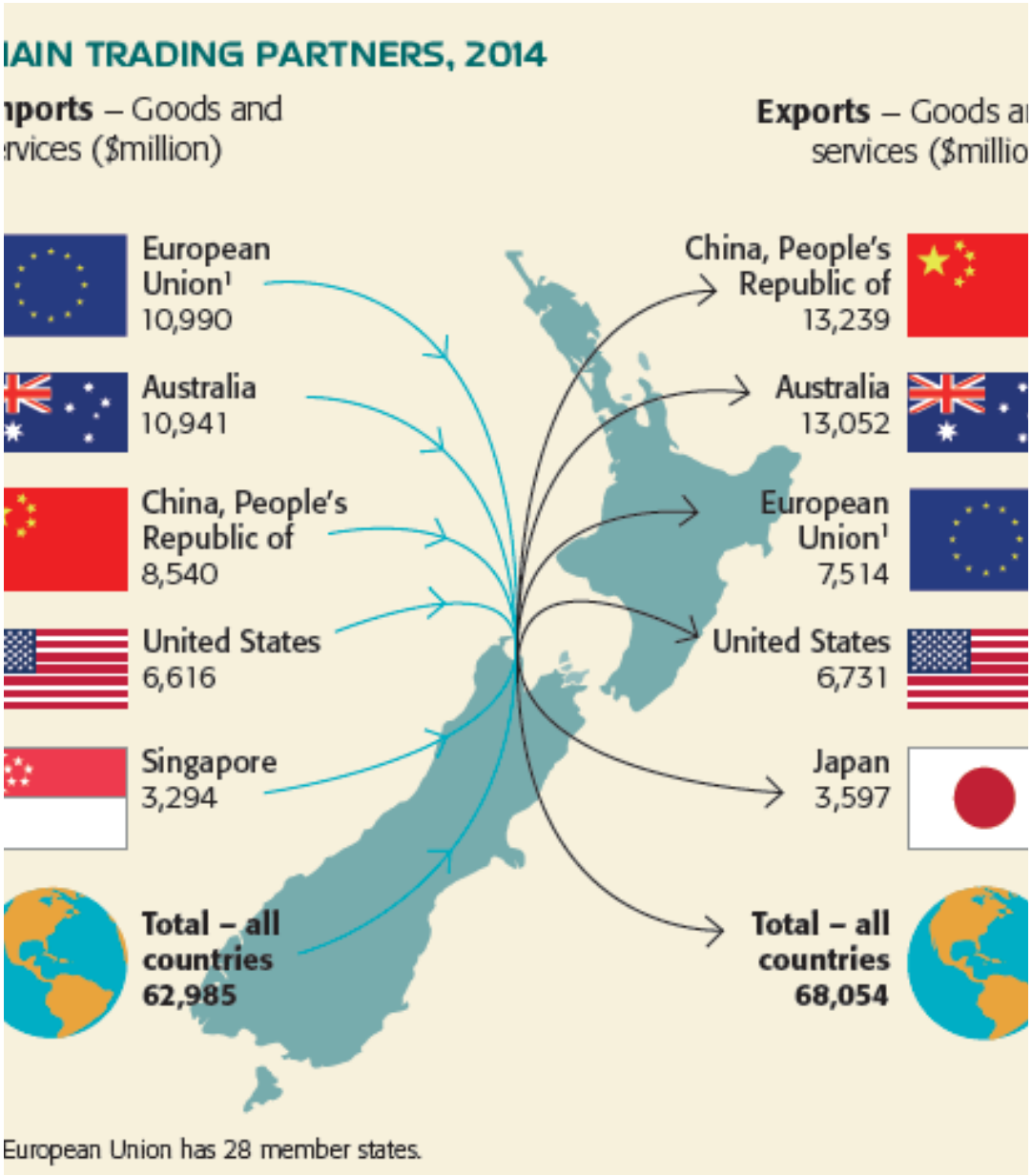
GARY HUGHES
BARRISTER

CHASING THE MONEY – ACROSS TRADING PATTERN BORDERS

NZ's largest trading partner figures 2015

NZ as a fraud exporter/producer? Or a fraud destination?

Payment in bitcoin



CHASING THE MONEY – how not to do it?

- Employment/HR − insider or staff member − the boss might call in the employment lawyer who prepared staff contract.
- Accounting irregularities uncovered - call in the usual financial accountant or auditor. Needed later to prepare evidential material, regularise the books, but won't get the money back.
- Police, FMA, SFO – criminal law important, but not mandated, resourced or prioritised towards getting the money back.
- Internal investigation − hush it up, keep the media out of it.
- Insolvency/liquidator proceedings – depends on company's precarious position, but usually too slow or public to preserve the stolen funds.

WORKING WITH, OR ALONGSIDE, OR SUBSERVIENT TO, GOVT LAW ENFORCEMENT?

Police, SFO, ASIC/FMA, ACCC/ComCom, Cyber and specialist agencies

Different objectives and statutory/political purposes

But wider and deeper powers of investigation (if you can persuade them to engage and to use it)

Crowding out of civil enforcement efforts – do they end up actually competing for the source of funds?

Criminal case takes priority, punishment and deterrence is the objective

GARY HUGHES
BARRISTER

Reacting to fraud: move fast, silently move decisively, and with specialist help

The single best chance of getting your money back is to immediately engage an expert fraud or asset recovery litigator – together with a specialist forensic accountant and an expert ~~hacker~~ digital demon.

GARY HUGHES
BARRISTER

Fraud and Asset Recovery - Team Approach

The suggested Co-ordinated Team approach:

- expert legal counsel – "asset recovery"
- specialist forensic accountant – asset tracing
- fraud investigators – research, find, surveil + snoop
- digital/IT experts – hire a … demon
- government enforcement/regulatory authorities
- property & valuation professionals, down the track
- HR & employment, PR & media, can follow later

GARY HUGHES
BARRISTER

A Strategic Approach to Asset Recovery

Stealth with Speed:

- Moving fast – investigate the facts, trace the person, bitcoin, bank account, wallet
- Move decisively − choose where to sue, hire a local expert, interim injunctions, urgent court orders
- Moving silently - Gags & Seals, no information leaks
- Freezing or seizing of assets on preliminary basis – holding orders, restraints pending final hearings
- Investigative orders/law enforcer – what else exists?

Internationally Co-ordinated Approach

Strategy needs to be aligned:

- Don’t have time to research who to hire
- Managing multi-jurisdictional cases and multi-disciplinary legal teams − retain legal privilege while sharing information
- Identifying likely locations of hidden assets, fraudsters or gatekeepers they use
- Getting ID info, tracing the wallet, finding the exchange, holder of crypto, or blockchain nodes
- Regulators compare notes, data, trends; inter-governmental mutual assistance agreements increasingly being used
- Strategy - where to initiate lawsuit to maximise results

The Legal Tool-Kit for Asset Recovery

Specialised Tools are available:

1. Mareva injunction (freezing order restraint)
2. Norwich Pharmacal, Bankers Trust, & other Disclosure orders: non-party, pre-commencement
3. Anton Piller orders (seizure & delivery up restraint)
4. Other Attachments/Charges, Restraints, Injunctions
5. Domestic/international criminal law enforcement agencies and regulators' investigative powers
6. Insolvency regimes and early use of powers
7. Tracing orders and Equitable remedies.

More in the Legal/Practical Tool-Kit

- Pre-action information gathering - tracing
- Investigative/examination tools and orders
- Third parties, non parties, banks, gatekeepers
- Public leaks – ICIJ, Wikileaks, OECD, tax authorities
- Use existing regulatory regimes (e.g. AML, anti-bribery, sanctions, self disclosure reporting)
- Trans-Tasman proceedings enforcement
- Tracing remedies; knowing receipt, or assistance
- Trust-busting techniques on the rise

Injunctions – in brief summary

- an order of the Court aimed at stopping a person from doing something, or making a party to do a specific act
- prohibitory or mandatory; as the name suggests
- traditionally, freezing bank account (prohibitory) was the way to go – mandatory injunction harder

Need a strong prima facie case against the person, or orders to attach to an un-named person

Usually can show plaintiff's interests have been damaged as a result of the hack/breach/rort

Strong affidavit evidence that person may flee, is in possession of incriminating evidence, or may transact/destroy the evidence

- Without Notice orders (undertakings to give to Court) then execute search orders on site(s)

Does the Tool-Kit work for virtual money?

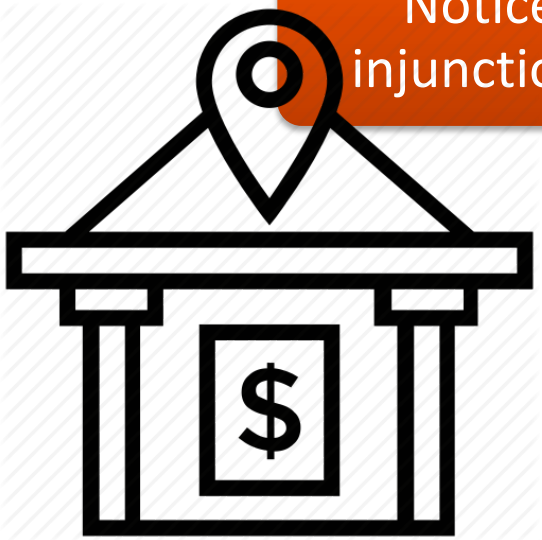
Partly – still need the pre-action information/tracing

- Disclosure and examination orders – locate a person/place/wallet/device – seize it, break it.
- Importance of the John Doe orders – ISP, telcos, fiat exchange, coin operator/exchange (now regulated?)
- Third parties, non parties, banks, gatekeepers, AML, or self disclosure reporting
- Equitable and legal remedies only the end game later, same with trust-busting orders
- Seizure and delivery up may be more important

GARY HUGHES
BARRISTER

Example application to virtual money?

Bitcoin → Wallet → Keys → Device/drive → Location ? → Without Notice injunction!



Networks – IBA Asset Recovery, ICC FraudNet

Global network of lawyers, formed around practice area specialties and expertise.

Representing business victims of fraud, corruption, asset theft and cyber or commercial crime.

Primary purpose - identify, freeze, and recover money, assets and proceeds of crime on behalf of victims.

Created at initiative of organisations like International Bar Assoc or International Chamber of Commerce.

Experts tend to know where other expertise resides.

IBA Anti-Corruption/Asset Recovery sub-group

- Voluntary, unpaid – but criteria set by members and the IBA objectives
- Sub-group of IBA professional body committee
- Only experts with established track record and significant experience are invited to act as officers
- Meetings and conference (knowledge-sharing) 2-3 times a year
- Highest ethical standards expected
- Provide public advocacy and thought leadership.

Who makes up deployment force?

- Lawyer members from over 90 countries – officers in different countries and roles
- Very broad global reach, a lot of activity around Africa and Asia
- Mostly experienced legal practitioners in fraud recovery and asset tracing
- Organised for immediate co-ordination, collaborative action and mutual assistance
- Avoid piecemeal, ad hoc and ineffective initiatives
- Assist to enforce local court freezing/confiscation orders

GARY HUGHES
BARRISTER

EFFECTIVE ACTION BY A SPECIALIST NETWORK: BANK CUSTOMER IDENTITY THEFT

IRELAND – ENGLAND – HONG KONG

8pm Friday evening, an Irish bank became aware of large amounts of money removed from a customer's account and transferred to the UK and then Hong Kong. Obvious to bank compliance/monitoring staff those transfers were not authorised payments.

9am Saturday morning, bank called in the Irish law firm Arthur Cox. During Sat-Sunday, various conference calls took place, AML and investigations were pursued into the UK and into the transaction data.

9am Monday morning, contact/co-operation with the Hong Kong bank that had received the unauthorised payments. Later that day instructions to a Hong Kong lawyer to prepare/obtain injunction.

Tuesday – barrister on feet in Hong Kong Court seeking urgent (without notice) application, successful result of a Freezing Order on the monies illegitimately transferred out of Ireland the previous Friday.

- Not counting the weekend, 48 hours to secure the funds!

GARY HUGHES
BARRISTER

US Fraud leads to Cook Islands

MULTI-JURISDICTION FREEZING & DISCOVERY ORDERS

- Large court judgment on fraud claim obtained originally in USA.
- Judgment debtor claimed to have no assets.
- Investigators for lead country law firm uncover evidence of luxury lifestyle and recent trust entity dealings in offshore jurisdictions, including Cook Islands.

- Evidence of fraudulent transfer of assets.
- Applications made in 5 countries, on co-ordinated basis, for freezing orders and Norwich Pharmacal/Bankers Trust disclosure orders (with confidentiality gags).
- Lawyers from NZ, support from CI FIU, Orders made by Cook Islands High Court (ie. a retired NZ Judge) other Orders elsewhere - without notice basis.

Seizure of Cryptocurrencies is beginning

BBC NEWS 21 JULY 2018

More than £1.2m worth of Bitcoins have been seized from a senior member of an organised crime gang.

Serejgs Teresko, 31, was kidnapped from a rented Virginia Water home in April 2017, where police found a large cannabis factory. He turned up later and a search found a crypto currency wallet used to access a Bitcoin account in his Cobham home.

He was jailed for nine years and three months for money laundering and drugs offences.

Following his arrest police found a keepkey device on which was stored £1.2 million worth of Bitcoin. They also discovered a number of bank and credit cards in multiple names, counterfeit European identity cards, expensive clothes, watches, jewellery and gold bars.

Police were given permission by the Crown Prosecution Service to convert the Bitcoin into Sterling and confiscate it under the Proceeds of Crime Act. Surrey Police said it was the first UK law enforcement agency to convert Bitcoin into Sterling and confiscate the money.

Rapid and Specialist Approach is key

- Global responsiveness is key – speed is everything
- Insurers very sensibly having 24/7 panel response
- Local point-of-contact service: for victims, to identify/investigate assets, execute recovery actions
- A network of experienced partners to investigate and take action against foreign fraudsters
- Increased odds of recovering money (finding wallet)
- Litigation funders in some jurisdictions inappropriate cases, access to financial assistance and innovative fee structures to pursue recovery

GARY HUGHES
BARRISTER

PRESENTER

Gary is a barrister providing advocacy & strategic risk management advice:

- specialising in all types of regulatory investigations and cases - Financial Markets Authority, Commerce Commission, Office of the Privacy Commissioner, AML/CFT Supervisors, other specialist regulators
- related privacy/data, corporate risk advice, and insurance law issues

Approved by NZ Law Society to take direct briefs (claims-handling, advice, mediation etc)

Gary has worked in insurance law throughout his career and his regulatory case-load engages Stat. Liability, Prof. Indemnity or D&O – increasingly cyber policy/response too.

Professional roles include acting as:

- ACAMS, the global financial crime organisation - NZ Programme Director
- International Bar Association - Anti-Corruption Division and Asset Recovery sub-committee, New Zealand country officer
- Author of the online text "*AML/CFT Workflows & Guidance for Lawyers*" on the Thompson Reuters WestLaw platform
- Honorary life member of LEANZ (Law & Economics Association of NZ), board member 2004-14

gary@garyhughes.nz
(+64) 021 477 780