

IFW  
GLOBAL

Presented by



Ken Gamble  
IFW Global Chairman



# Operation Tropicana

## Malaysia, *Feb 2023*



FINANCIAL CRIMES  
IN AUSTRALIA

Unmasking Fraud, Corruption & Money Laundering  
Managing Risks in the Digital Age

3 June 2025  
Amora Hotel, Sydney

5564488866650805  
0193642667390905  
490917167381159001  
76673550784399346  
17617927735625346  
823810794447071177  
01102304389805453  
5564488866650805  
0193642667390905  
490917167381159001  
76673550784399346  
17617927735625346  
823810794447071177  
01102304389805453  
5564488866650805  
0193642667390905  
5564488866650805  
0193642667390905  
490917167381159001  
76673550784399346  
17617927735625346  
823810794447071177  
01102304389805453  
5564488866650805  
0193642667390905  
5564488866650805  
0193642667390905  
490917167381159001  
76673550784399346  
17617927735625346  
823810794447071177  
01102304389805453  
5564488866650805  
0193642667390905  
5564488866650805  
0193642667390905  
490917167381159001  
76673550784399346  
17617927735625346



# WHO IS IFW GLOBAL



**Ken Gamble**

**Executive Chairman**

**Location**-NSW,Australia

**18 years with IFW Global**

Ken is a front-line cybercrime investigator with extensive qualifications and experience in investigation, intelligence, surveillance and asset recovery, developed over a 37-year career. Ken has consulted to various foreign governments and law enforcement agencies and presented on cybercrime topics at Interpol events. Ken has received 4 law enforcement awards



**Allan Watson**

**Director of Global Investigations**

**Location**-United Kingdom

**18 years with IFW Global**

Allan Watson has 40 years' experience in varying fields of investigations. These include serious investment fraud, asset tracing and recovery, business intelligence and security and crisis management in both the corporate and government sectors. Allan is presently in charge of coordinating complex investigations in many continents across the world including Asia, Europe, Africa, Middle East and the Americas.





# Background of Operation Tropicana

- Landmark transnational investigation exposing a \$1 billion investment scam run from secret call centres in Malaysia
- Led by IFW Global in collaboration with the Malaysian Anti-Corruption Commission (MACC) in a private-public partnership
- Over 80 suspects arrested across 24 simultaneous raids in Kuala Lumpur and Johor (Penang)
- Sophisticated fraud network targeting global victims with fake IPOs and share investments
- Complex laundering of criminal proceeds through banks in Hong Kong, Thailand, and Singapore
- Infiltration by IFW operatives provided covert intelligence to dismantle the network
- Major breakthrough in targeting "professional enablers" within financial institutions





# THE IPO SCAM

- The scammers heavily promoted IPOs on Australian social media platforms. *An IPO is the process of offering shares of a private corporation to the public in a new stock issuance for the first time.*

*The fraudsters used IPOs of real companies*

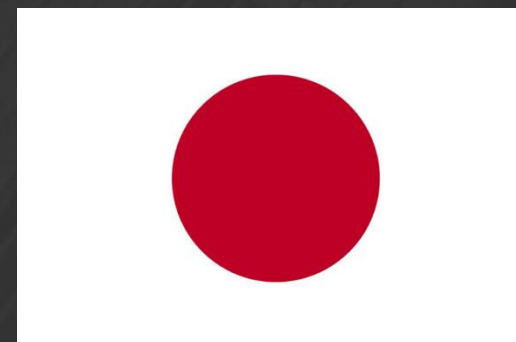
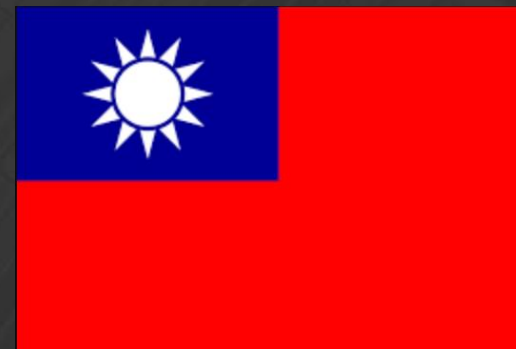
- ASM Pacific Technology
- Space X IPO
- Energy Australia
- Porsche IPO
- Starlink IPO
- Apple
- Hyper Vision Limited
- Rivian Automotive Electric Vehicles
- Xiaomi IPO
- Tesla
- Novacure





# Virtual companies operating slick websites from Japan, Taiwan, Hong Kong promoting real IPOs

- \* Agard Union Trading
- \* Aspen Asset Management
- \* Lincoln Management Group
- \* Charrington Pacific Group
- \* Cullman Mutual Capital
- \* Kingsman Investments
- \* Tochigi Mutual Capital
- \* Chiba Taiko Partners
- \* Suncap Advisors
- \* Whiteoak Capital



# Charrington Pacific Group Announces Implementation of New Technology Platform

NEWS PROVIDED BY

[DELETE](#)

April 01, 2021, 11:33 GMT

SHARE THIS ARTICLE



*Charrington Pacific Group, has announced today the launch of a new digital wealth management platform for its workforce.*

TOKYO, JAPAN, April 1, 2021 /[EINPresswire.com](#)/ -- [Charrington Pacific Group's](#) platform is designed to power a modern wealth management business – including functionality to streamline internal processes. Features include proposal generation, paperless onboarding, risk-questionnaires, model management software, client portfolio monitoring and rebalancing tools, fee billing, compliance tools and a client portal.

## Contact

Martin Seon  
Charrington Pacific Group  
+81 3-4563-8944  
[martin.seon@cpgroupcorp.com](mailto:martin.seon@cpgroupcorp.com)

## More From This Source

[Charrington Pacific Group Announces Implementation of New Technology Platform](#)

Scams promoted  
worldwide on self  
publishing newswire  
websites



# The Money Laundering



- After victims agreed to “invest”, they were directed to make wire transfers to bank accounts that they were told were “escrow accounts” held by “Transfer Agents” in, among other places: Malaysia, Hong Kong, Singapore, UAE and Indonesia.
- These “escrow accounts” were held by shell companies created by the suspects to further the investment fraud scheme and launder the proceeds.





## The Protection Racket

- IFW operatives uncovered a KL based security company protecting the fraud group
- The security company was owned by former high-ranking members of the Royal Malaysia Police
  - titles
- A middleman named Mr. "K" was the "go-between" and "Enforcer" paying USD50K a month for protection



# The Enforcer & Protector

- **Permal Kunder A/L KARUPAN** leased residential apartments on behalf of Boiler Room Foreign workers to reside in whilst in Malaysia.
- Many of these were Filipino workers, trafficked into Malaysia under false employment letters.
- The workers passports were confiscated once they were in Malaysia and held by management as “security” over the workers
- Workers were told the operation was protected by Police and AMANATS Security and anyone who leaked information would be dealt with harshly





# The Sources

- IFW recruits a source who was previously employed in the boiler room to provide details of the office locations and floor layout
- IFW operatives' recruit a second source to work in the boiler room undercover to gather evidence and intelligence on the group







The boiler  
room fraud  
offices





## The approach to Chief Commissioner of MACC in 2022





MACC Launches Operation Tropicana

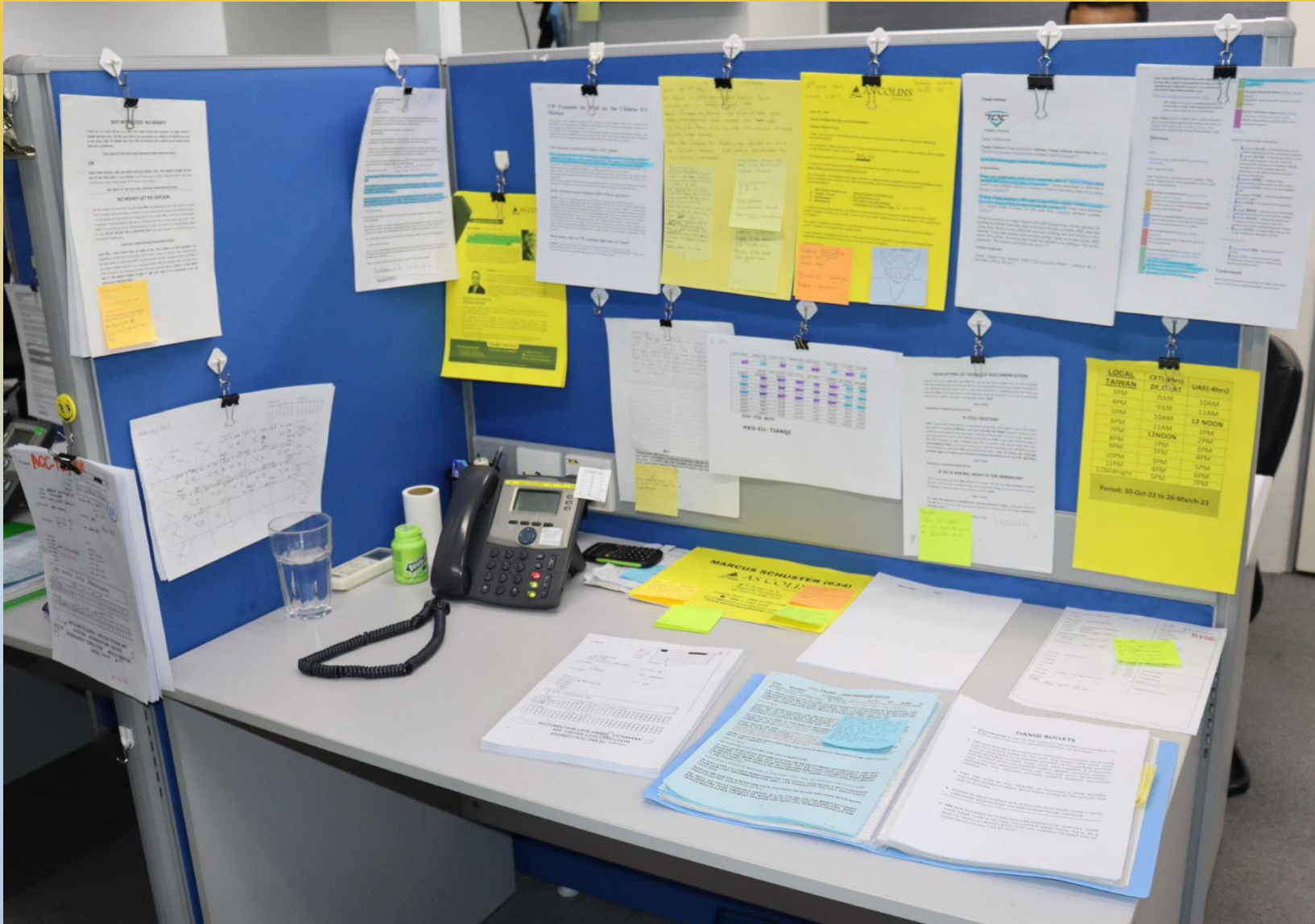


# The Strike – 21 FEB 2023

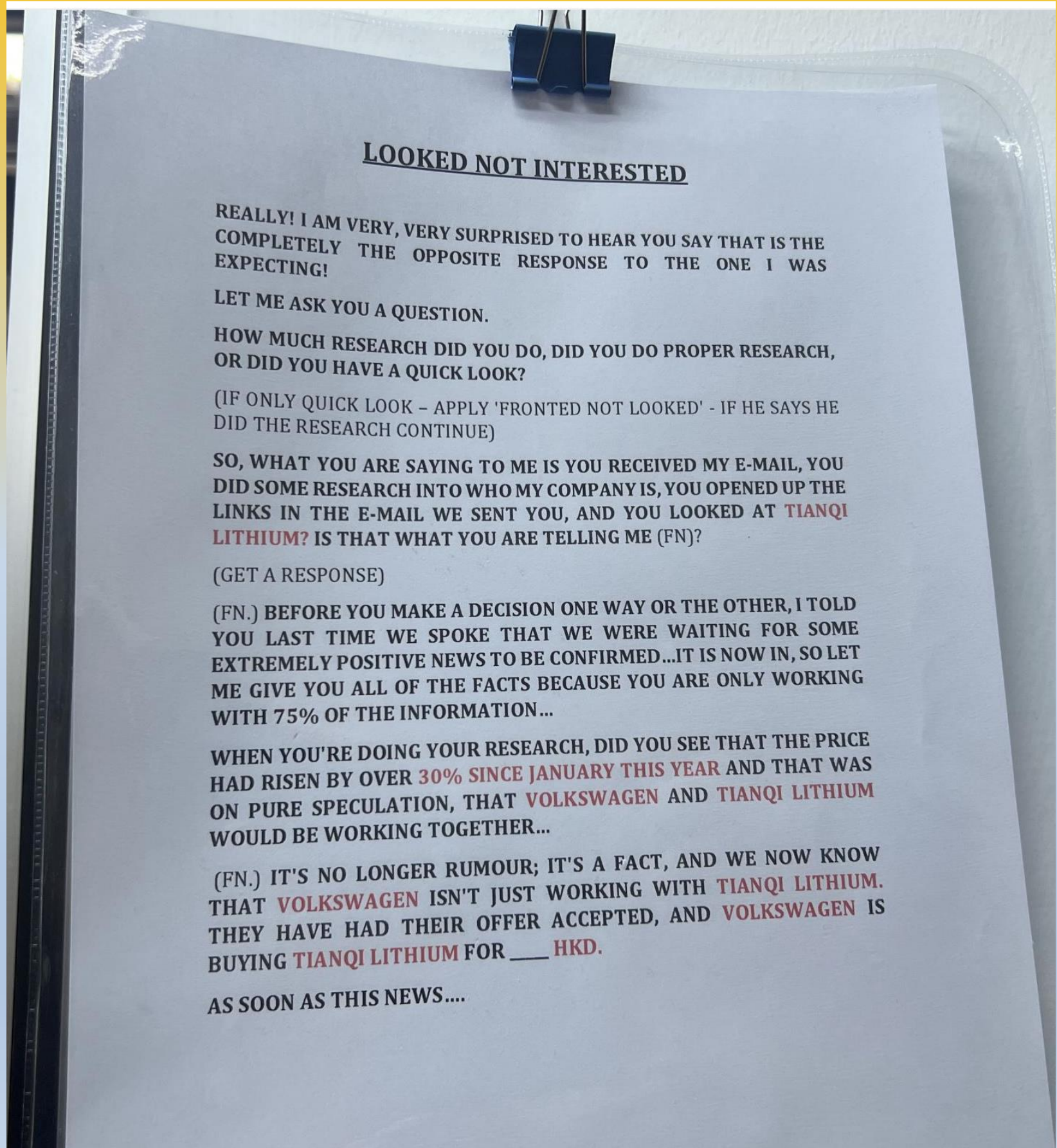




# The Scripts



A treasure trove of scripts and documents on how to scam investors





# The Arrests







SPOTLIGHT 



# THE SEIZED ASSETS





# The Seized Assets





# The Fraud Mastermind

Andy Peters *aka* PegLeg

- 52-year-old **British citizen**
- **Wanted** by UK authorities
- Running Boiler rooms in SE Asia for **20 years**
- Amassed significant wealth
- Closely **connected to Organised Crime** Groups in Thailand, Philippines, Russia and China
- **Pleaded guilty** and served **only 6 months** for one charge
- **Back in business** targeting Australians again since early 2024





# The Result



- **81 arrests** of boiler room investment scammers
- **24 search warrants** simultaneously served
- Equivalent to **AUD 4.3 million** in cash seized
- **54 bank accounts** frozen
- **20 bank employees** questioned
- **170 Officers** involved (No Malaysian Police involved)
- Caught in the act of setting up crypto scam office with 200 employees
- **Major disruption** to organised fraud against Australians

## OPERATION TROPICANA

Malaysian Anti-Corruption  
Commission (MACC)

Kuala Lumpur, Penang,  
Malaysia

21 February 2023



# The Malaysian Banks

## *Key Compliance Failures Identified by IFW Global*

### Bank Number 1

- Failure to conduct Enhanced Due Diligence (EDD) despite multiple high-risk indicators
- Accepted accounts using **generic Gmail addresses** instead of corporate domains
- No verification of legitimate business operations or physical site visits conducted
- Ignored clear **money laundering typologies**, including rapid personal deposits and withdrawals
- Relied on **unverified or duplicated documents** with questionable certifications
- Failed to escalate geographic risks related to **offshore operations** (Indonesia & Philippines)
- Account activity showed **no linkage to declared clients or business services**
- Inconsistent or **fabricated operational details**, including mismatched addresses
- **No Suspicious Transaction Reports (STRs)** were filed, despite overwhelming red flags
- Systemic breach of Malaysia's **AMLA 2001 obligations** and Bank Negara compliance standards





# The Malaysian Banks

## *Key Compliance Failures Identified by IFW Global*

### Bank Number 2

- Approved a **“High Risk” corporate account** without conducting Enhanced Due Diligence (EDD)
- Failed to independently verify **residential or business addresses** of directors or premises
- Allowed a **foreign sole signatory (Chinese national)** to control the account despite a local co-director
- Accepted **fabricated supporting documents**, including a suspicious payslip and business records
- **No Tax Identification Number (TIN)** was provided or followed up during onboarding
- Approved a **USD \$1 million foreign exchange facility** with no matching business justification
- Did not obtain **prior personal or corporate banking history** to validate financial legitimacy
- Overlooked use of a **generic email address**, contradicting corporate governance standards
- No site visits, no operational legitimacy checks, and no escalation to **Financial Crime Risk teams**
- Breached Malaysia’s **AMLA 2001** and Bank Negara guidelines by enabling illicit fund movement





# The Malaysian Banks

## *Key Compliance Failures Identified by IFW Global*

### Bank Number 3

- Approved multiple high-risk corporate accounts without performing **enhanced due diligence (EDD)**
- **Failed to verify beneficial ownership, director residency, or operational legitimacy** for foreign-incorporated entities
- **Accepted falsified, incomplete, or unverifiable documentation**, including fabricated contracts and missing TINs
- **No site visits conducted** and improper waivers used to bypass mandatory inspections
- **Allowed use of generic email accounts** and failed to question missing websites or corporate domains
- **Repeated use of same address and introducers across multiple fraudulent entities** was not escalated
- **Permitted rapid in/out fund movements from personal names**, inconsistent with declared business activity
- **No Suspicious Transaction Reports (STRs) filed** despite clear laundering typologies
- **Same relationship managers onboarded multiple linked fraudulent entities** without raising alerts
- Closed accounts quietly without investigation or documented rationale, violating AMLA and FATF standards





# The Malaysian Banks

## *Key Compliance Failures Identified by IFW Global*

### Bank Number 4

- Failed to verify director identity and residency under Labuan and Malaysian regulatory requirements
- Approved accounts without valid business license, operating agreement, or evidence of trading activity
- Accepted **generic email addresses** and lacked verification of digital or corporate presence
- **No supporting documentation for financial claims**, including unsubstantiated million-dollar revenue projections
- Allowed onboarding based on **remote notarisation** without confirming applicant presence in Malaysia
- **Ignored adverse credit and regulatory red flags** during background checks on directors
- **No site visits conducted**, and waivers were undocumented or unjustified in breach of internal policy
- Allowed **layering transactions**: rapid movement of funds from unrelated individuals without commercial link
- **Failed to obtain and retain mandatory KYC documents**, including passport and address proof
- **Closed accounts without filing Suspicious Transaction Reports (STRs)** or providing reasons for closure





# The Malaysian Banks

## *Key Compliance Failures Identified by IFW Global*

### Bank Number 5

- Approved corporate account for high-risk entity **without Enhanced Due Diligence (EDD)**
- **Failed to verify declared business operations**, allowing fictitious crypto advisory claims
- Accepted **generic Gmail address** and unsupported business website as legitimate contact points
- **No inspection of premises** or validation of claimed business location in Kuala Lumpur
- Permitted a **Chinese national to be sole operator** of Malaysian company without confirming local substance
- **No evidence of historical financial records** or business activities at time of account approval
- Overlooked **inconsistent director records and rapid corporate structure changes**
- **Allowed rapid third-party deposits and withdrawals** without questioning source or legitimacy
- Did not escalate or report **blatant laundering typologies**, contrary to AMLA and Bank Negara standards
- **Relationship manager failed to question high-risk indicators**, enabling fraudulent fund flows





**“If this is what we  
uncovered... imagine what  
still lies hidden.”**

*– Ken Gamble, IFW Global*





A leading  
global  
cybercrime  
investigation  
agency

Contact Information

**Ken Gamble**

**Executive Chairman - IFW Global**

**Board of Directors- International Association of  
Cybercrime Prevention (IACP)**

**Tel: + 0412 433 888**

**E: [kgamble@ifwglobal.com](mailto:kgamble@ifwglobal.com)**

**[www.ifwglobal.com](http://www.ifwglobal.com)**