CASE SUMMARY

Zschimmer & Schwarz GmbH v Persons Unknown & Anor

High Court grants proprietary and Mareva injunctions, substituted service by email, and Malaysia's first Spartacus Order against anonymous cyber fraudsters

⚖️ **Rules of Court 2012 & English case law**

Facts

In September 2020, a German chemical manufacturer, Zschimmer & Schwarz GmbH, was tricked into instructing its bank to pay a commission of approximately €123,000 into a Malaysian bank account. Unknown persons had infiltrated the company's email exchanges, impersonated its long-standing South Korean business partner, and intercepted courier-shipped verification forms. The fraudsters manipulated those forms to change the payee bank details to a Malaysian Muamalat Bank account. The German bank, however, stopped the payment for further authentication. Undeterred, the fraudsters tried again. They provided new bank details — this time for a CIMB account held by Mohammad Azuwan bin Othman, trading as Premier Outlook Services — and once more manipulated the courier-based verification process. On or about 27 October 2020, the company instructed its bank to pay approximately €123,014.65 into the CIMB account. The funds were credited on 30 October 2020 and fully transferred out shortly thereafter. The real perpetrators — referred to in the proceedings as "Persons Unknown" — could not be identified.

The company applied urgently to the Kuala Lumpur High Court for relief against the unknown fraudsters and the known account holder.

Legal Issue

Whether the High Court could grant a proprietary injunction and a Mareva freezing injunction against "Persons Unknown"; whether substituted service of court papers could be effected via email and a Dropbox link; and whether a self-identification order (Spartacus Order) could be made requiring the anonymous fraudsters to reveal their identities.

Held (High Court, 22 December 2020 & 13 February 2021)

Judicial Commissioner Ong Chee Kwan granted all the reliefs sought. The court held that:

- A proprietary injunction and Mareva freezing injunction could be issued against "Persons Unknown" who were identifiable by reference to their actions — namely the email addresses they used and the bank accounts they controlled.
- Substituted service of the originating process on the 1st Defendant could be effected via the fraudulent email addresses, with a Dropbox link to the full cause papers because the documents were too large to attach.
- Malaysia's first Spartacus Order was granted, requiring the unknown fraudsters to identify themselves by responding to a newspaper advertisement within seven days, failing which they could face committal for contempt.
- When the funds were traced to other bank accounts, further injunctions were granted against the new recipients, confirming that the remedies could follow the money.

Key Reasoning

- The court drew on English case law, particularly *CMOC Sales & Marketing Ltd v Persons Unknown* [2018] and the two-category test in *Cameron v Liverpool Victoria Insurance Co Ltd* [2019], which distinguishes between anonymous defendants who are identifiable (Category 1) and those who are truly unidentifiable (Category 2). The fraudsters fell within Category 1.
- Nothing in the Malaysian Rules of Court 2012 prohibited filing claims against "Persons Unknown"; Order 89 of the Rules already

permitted such references in land possession cases, providing a procedural foothold.

- The court also cited a Malaysian legal text, *Foong's Malaysia Cyber, Electronic Evidence and Information Technology Law*, reinforcing that local legal writing supported the approach.
- The purpose of the injunctions was to act as a springboard for further disclosure orders, with the goal that the fraudsters could eventually be identified.

Practical Significance

Victims of cyber fraud in Malaysia can now seek urgent freezing orders even when the perpetrators are unknown. Injunctions can follow the money across accounts. Substituted service via digital channels is available, and a Spartacus Order can compel anonymous defendants to come forward. The case underscores the importance of a swift cyber-fraud response: freezing assets, preserving all evidence, and applying for urgent court relief. Businesses should have a cyber-fraud response plan in place that includes immediate legal steps.
