Know Your Employee

Know Your Employee

Marius Frunza • IntelBlitz • 6 mins read • Oct 1 2021

How well do you know your employees?

In the age of remote/hybrid work, onboarding and monitoring employees have become challenging tasks for every corporation. The main narrative of compliance officers relies on the postulate that critical threats stem from external agents, such as clients, suppliers or competitors. What are the particularities of a comprehensive “Know Your Employee” (KYE) process?

KYE allows secure employee onboarding and gives management a fully-fledged picture of employees’ backgrounds. KYE, as a process, does not stop once the worker is hired but continues to monitor the employee’s status. In the new remote/hybrid work environment, five key areas could potentially generate unforeseen exposure to fraud risk.

Overemployed

Working two or more jobs simultaneously was an ephemeral dream for many workers who feel underappreciated in their careers. However, the lockdown, the digitalisation of the economy and the remote work policies opened the gate to spinning multiple jobs. There is even a platform dedicated to such multi-jobs employees. Overemployed.com is a community of professionals looking to work two remote jobs, earn extra income, and achieve financial freedom. Many testimonies underlined that agile workers could hold up to five jobs, including prominent roles with global corporations. Needless to say, that for a significant corporation employing people non-exclusively is not compliant with their internal policies.

Protecting IP

Many startups or innovative companies hiring people remotely might face huge risks related to intellectual property. Remote

workers can easily replicate an idea or an innovative technology for their own benefit. If those employees are based in a different jurisdiction, the employer would not have the upper hand in litigation with a remote employee who misused the company's IP.

Social media activity

An office-based work environment allows the employer to filter the type of communications employees can have during working hours. Company internet connection may curtail access to persona email and social media. Thus, employees' communication through web-based infrastructure using the company's infrastructure is kept to a minimum. For a remote worker, it is much more difficult to filter or control communication through social media. Thus, a remote employee can disseminate during working hours.

Insider trading

Regulated financial markets activities faced unprecedented risks during the lockdowns triggered by the coronavirus pandemic. Trading floors in reputed financial institutions have a high level of security to avoid all types of leakage of confidential private information. However, when traders, market-makers and brokers work remotely, the level of control is to a lesser extent. This opens the gate widely to market abuse because confidential information can easily be disseminated out of the professional environment and leaked to people from employees' networks who can use it for their own benefit.

VPN

While remote work may be the right choice for many companies, knowing precisely the employee's location and the fact that the employee himself is fulfilling the tasks are not negotiable. VPN solutions can hide the real location of the employee and disguise the identity of the person who does relly the work. Such aspects are critical for companies working with clients' data, whereas the data privacy regulations are different depending on the jurisdiction where data is effectively processed.

"Digital surveillance programs require concrete data centres; intelligence agencies are based in real buildings. Surveillance systems ultimately consist of technologies, people, and the vast network of material resources that supports them."

Trevor Paglen, American artist

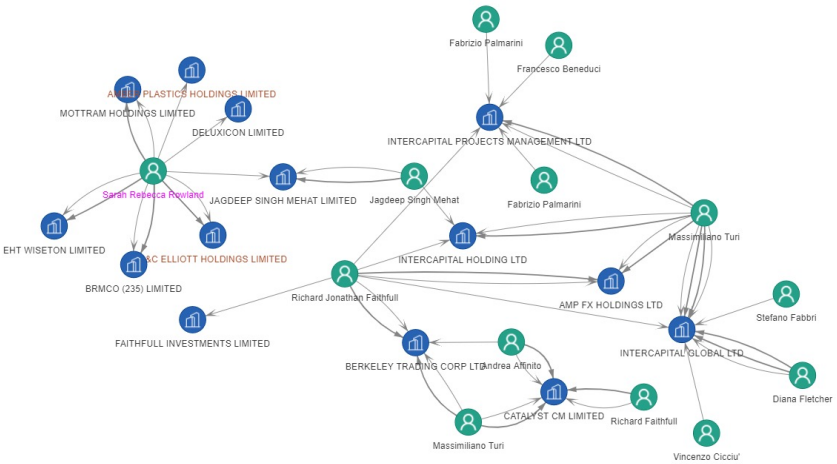
Focus: Richard Faithfull

Engineering money laundering

Richard Faithfull (DOB: 15.03.1990) was sentenced in early September to 5 years and 10 months imprisonment for laundering money and was also disqualified from being a company director for a period of 10 years. Following an investigation by the Financial Conduct Authority and the City of London Police Faithfull was brought in front of the Westminster Magistrates Court in January 2021. According to prosecutors, Richard Faithfull laundered 2.5 million GBP as part of a transnational organised crime group for longer than 12 months between 1 June 2017 and 1 August 2018, laundering the proceeds of, at least, 7 investment frauds based overseas. Faithfull controlled a network of UK-based companies with ties in Italy and Canada. He used these firms to deploy his money laundering strategy.

Faithfull worked in the regulated financial services sector - as an investment advisor. Thus he used use knowledge gained in the industry to help fraudsters to dissimulate the proceed of their crimes. The FCA investigation showed that his network of companies was paying fictional 'dividends' from bank accounts controlled by him to make it look as though the underlying investments were generating returns.

When law enforcement started to put pressure, he moved to Ukraine to avoid prosecution. He continued his illegal activities from overseas relying upon innocent parties to help him with operations.



Case Study: Richard Faithfull

Word on the street: Colombo administration indicted

Mafia boss in jail

The FBI continues its crackdown on New York's underworld. In mid-September, 14 mobsters were charged with labour racketeering, extortion and money laundering in a big scale operation that resulted in the arrest of Ten members of the Colombo crime family and one member of the Bonanno crime family. Colombo crime family boss Andrew "Mush" Russo, underboss Benji Castellazzo and consigliere Ralph DiMatteo were the most prominent figures amongst those indicted by the federal agents. According to the prosecutors instructed in this matter underlined the members of the Colombo family attempted to shake down union leaders and its affiliated health care fund to extort more than 10,000 USD per month to their own interests. According to the Department of Justice, the defendants can face up to 20 years in prison.

Know Your Network, AI meets KYC

More insights at schwarzthal.tech

Marius Frunza
marius.frunza@schwarzthal.com

The information and data published in this newsletter were prepared by the market research department of Schwarzthal Tech

Contact

contact@schwarzthal.com
FR: (33) 6 27 29 78 34
UK: (44) 7 95 22 08 734
RU: (44) 7 95 22 08 723

Address

Devonshire House, 582 Honeypot Lane,
Stanmore, England,
HA7 1JS

Social

twitter.com/schwarzthal

linkedin.com/company/schwarzthal-tech