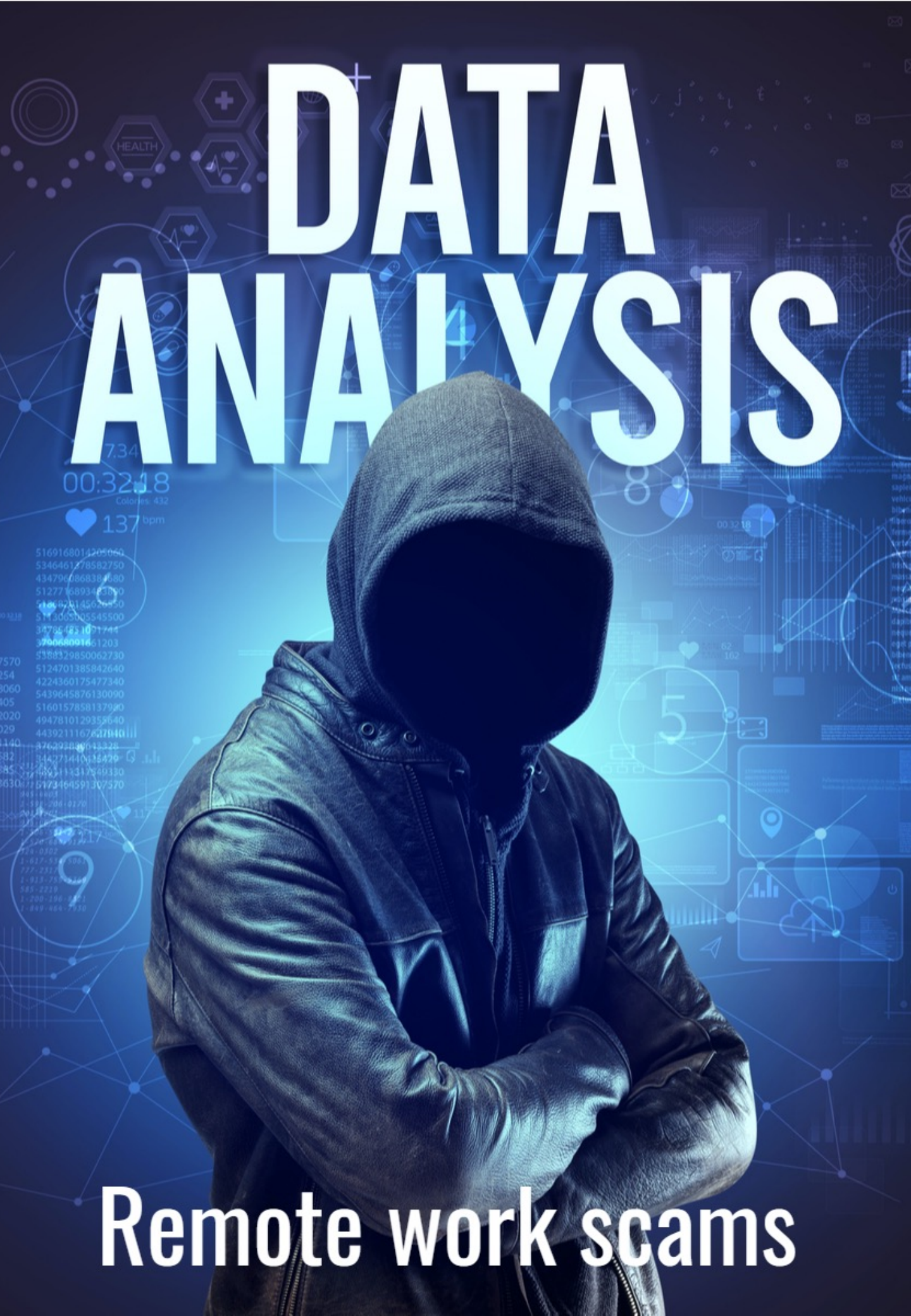
DATA
ANALYSIS
Remote work scams

Remote work scams

Marius Frunza • IntelBlitz • 4 mins read • Jan 21, 2022

Remote work and remote con

While tech entrepreneurs dream about virtual workspaces in a future enterprise Metaverse, the current state of remote work is grim. Two years into the pandemic, companies have learned to deal with their employees working remotely. Nevertheless, remote work scams spread faster than the new coronavirus and touched many firms regardless of their size and sector. So what are some cruel realities of remote work?

During the initial lockdown, remote work was supposed to be transitory, but it became the norm by the end of 2020. Most economic sectors went through an accelerated digitalisation path, thereby facilitating remote work. Tech companies led the way and encouraged their staff to work from home extensively. But, things went out of control when new employees were hired remotely, and even new companies were founded through remote work without any physical interaction.

Remote recruitment is tricky

While moving from office hours to remote work is a relatively simple task in a tech company, hiring new staff is a more complex endeavour, especially for small and medium companies. Scammers mainly target small firms that cannot compete with big corporations for highly skilled workers and have fewer means for screening candidates. Technical interviews over Zoom and online tests are tricky because candidates can easily fake them. Moreover, those scammers-candidates are playing a short-con. They get hired, take a few months of remuneration, and ultimately are sacked. Afterwards, they find another target and rerun the con.

Plenty of capital, not enough staff

COVID-19 generates a massive paradox. While in the previous crisis, there was a shortage of liquidity and a workforce excess, during the current pandemic, there is an enormous inflow of capital and a shortage of staff. The primary beneficiaries were tech companies that triggered a recruiting frenzy. Workers and tech specialists, in particular, realised that they had the bargaining power. Start-ups from Silicon Valley with huge funding rounds were desperate to hire people to keep up with their roadmaps.

Too many full-stack developers

In less than one year, the number of Linkedin profiles labelled as full-stack developers or data scientists increased exponentially. The total number of tech students worldwide would not suffice to explain this apparent inflation in supply. In reality, many of the new tech talents are scammers. Individuals with no technical background understood that there was money to be made in the tech sector. Moreover, they understood that start-ups have limited capacity to vet them properly.

Russian became overnight a global language

The investing frenzy in tech firms increased the demand for IT specialists, such as full-stack developers, data engineers, DevOps, UI/UK… However, in the world of tech, the trend is toward subcontracting the development in Eastern Europe, with a propensity for Russian-speaking countries, where the price-quality ratio is optimal. Therefore, many con artists create synthetic profiles claiming they are based in the ex-Soviet bloc.

It is not unusual to spot a certain Vladimir Kim or Natasha Igorov, holding BSc degrees from American universities offering freelance services from Russia. They are not, in fact, Russian, do not speak Russian and have never been there. They are, in most cases, based in South Asian countries claiming a fake nationality to increase their rates.

Data privacy: A headache for employers

Some companies put in place surveillance systems for their remote workers, but data privacy laws are a hindrance. In addition, remote work conflates the worker's personal life with the professional activity. This prevents companies from fully-fledged surveillance of remote work activity.

" The future we envision for work allows for infinite virtual workspaces that will unlock social and economic opportunities for people regardless of barriers like physical location. It will take time to get there, and we continue to build toward this."

Andrew Bosworth, VP Facebook Reality Labs.

Focus: Penalties fell in 2021

USD 5.4 billion

The amount of penalties issued over money laundering, KYC and data privacy to the financial services industry plunged by 50% in 2021, accounting for USD 5.4 billion.

The Fenergo estimate showed a significant contraction compared to 2020 when global financial institutions were hit with USD 10.6 billion. Moreover, the total number of fines issued by watchdogs declined from 760 in 2020 to 176 in 2021.

British regulators had a productive year and boosted nearly threefold the amount of penalties inflicted in 2021 with a total of USD 688 million compared to USD 231 million in 2020.

Analysts attribute the overall decline in penalties to the coronavirus pandemic that hindered the investigation processes. As a result, regulators and law enforcement were forced to depend mainly on digital investigations, thereby limiting the scope of their findings.

Nevertheless, this could show that regulators may look in the wrong place. Money launderers moved to new harbours and used fintech, digital payments infrastructures and crypto-currencies. Unfortunately, these sectors are still below the radar of watchdogs.

Amongst the prominent banks hit with penalties, we note:

- UBS: Swiss bank UBS was hit with a USD 2 billion fine by a Paris court for helping wealthy French clients to hide their wealth from tax authorities.
- Natwest: The reputed British banks were slammed by the FCA in December 2021 with a USD 350 million fine for insufficiencies in their efforts to tackle financial crime
- HSBC: The Honk Kong-based institutions had a USD 85 million fine

The word on the street: Nigerian mafia

A new threat

Italian police arrested last week four suspected members of a powerful Nigerian gang known as *Black Axe*, considered a rising organised crime syndicate by the authorities. Law enforcement operated the indictments in the south of Italy in the Sicilian capital Palermo and Taranto in the region of Puglia after receiving information from a victim of human trafficking.

Black Axe is a cult-like criminal gang that emerged in the 1970s at the University of Benin. The gang operates globally in several European countries and specialises in human trafficking and prostitution. The gang uses traditional Nigerian occult beliefs to inflict fear on their victims. For example, women forced into prostitution undergo a ritual called “juju”, which binds them to their traffickers.

There is limited intelligence on this gang, but various reports show that the organisation is, in reality, much stronger.

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