



## *Money Laundering Misconceptions:*

# The 7 Myths Every MLRO Should Know

If you work for a financial services institution, there's an 85% chance that right now your company is breaking the law. Whilst no respectable financial institution or employee wants to deliberately breach legislation, as any lawyer will tell you, ignorance of the law is not a defence - especially when it's a fundamental part of your job.

### Myth 1:

"We are a UK company and JMLSG/EU 3MLD says you must only be aware of Foreign PEPs."

Put the JMLSG/EU 3MLD aside for a moment. Your existing legal obligations under current UK legislation, such as the Prevention of Terrorism Act and the Proceeds of Crime Act, specifically state that it is a criminal offence for a firm to be involved in a transaction that involves the proceeds of crime, or a transaction that is funding terrorism. You must regularly screen your customer base to identify suspicious individuals and activity.

### Myth 2:

"All our customers are fine, upstanding UK citizens, so we're low risk."

Several of the 7/7 London bombers were also all 'fine upstanding UK citizens' on paper, yet had direct links to Al Qaeda. How people present themselves is not necessarily who they really are, and it is naive to operate your business on such an assumption.

### Myth 3:

"We have never had an issue with any of our customers being on the Bank of England sanctions list."

The Bank of England, FSA and Home Office lists contain the barest minimum of names and fall considerably short of your legal obligations. For example, on all the regulatory lists globally there are approximately 1,000 unique terrorist / terrorism names. Without screening your client base against comprehensive lists you are operating blind because you simply do not know if you are dealing with these people.

Anybody thinking of playing Russian Roulette with Watch & PEP lists should bear in mind that one leading 3rd party list provider estimates their total file will contain over half a million names by the end of this year.

A surprising number of MLROs make assumptions about legislation and unknowingly infringe it, leaving themselves open to serious risk and exposure. Most of these assumptions stem from seven myths about anti-money laundering measures.

Simon Pearson,  
Director of  
Client Screening,  
Datanomic

## Myth 4:

**"We have a very low risk profile/ We only deal in standard retail investments like ISAs etc - 'bad guys' don't want those products."**

Just because you provide 'low risk' retail financial products such as current or savings accounts, ISAs, PEPs and Pensions, doesn't mean your customer base is low risk.

In screening more than 300 million customer records Datanomic has routinely discovered organized criminals, financial criminals, suspected terrorist financiers and other 'bad guys' as customers of leading UK retail banks, life & pensions providers, asset managers and investment companies. Also, contrary to popular opinion, your risk profile is far higher for UK mainland business than it is for offshore.

## Myth 5:

**"We check them on new account opening and once/twice per year thereafter - which is sufficient to meet regulatory requirements."**

There's an enormous difference between doing the absolute

minimum - going through the motions of putting a tick in the box - versus taking pro-active, responsible steps to professionally mitigate risk for your institution.

Exposure to risk, criminal prosecution of a bank's senior management, hefty financial fines and penalties and reputational damage don't just happen twice a year. Risk is an ongoing, ever increasing and escalating occurrence, which is why companies such as Datanomic make it easy to conduct regular, automated screening on the very latest intelligence. Screening individual customers two out of every 365 days leaves you completely exposed.

## Myth 6:

**"We have a small customer base of a few hundred thousand customers - and we know them all personally."**

Unsurprisingly, criminals do not wish to be easily identified. By their very nature, they do not want to be found. So, despite the growing number of names on the lists supplied by the likes of Bank of England and OFAC (United State's Office of Foreign

Asset Control) they are becoming increasingly difficult to identify when hidden in a large corporate database.

Whilst some criminals resort to identity theft and forged passports to cover their tracks, others simply manipulate their own names and personal details to create multiple personae, opening accounts under aliases or spouses names.

## Myth 7:

**"We are a private bank dealing with wealthy individuals. Our account managers know clients well enough to determine if they are criminals or terrorists."**

Just because a customer is wealthy does not mean they don't have anything to hide or are above breaking the law. The assumption that the higher the wealth, the lower the risk is not only irresponsible, it is also untrue. Some of the wealthiest individuals in the country are wanted by the Serious Fraud Office for crimes ranging from insider trading to multi-million pound price fixing scams, to name but a few.

## Conclusion:

The latest European legislation, the EU 3MLD, which became law on 15 December 2007, stipulates that firms must have "effective systems and controls" in place to screen for money launderers, terrorists, terrorist financing, criminals, PEPs et al. Checking customers twice a year or when they open a new account is not an effective system or control. Assuming high net worth individuals or customers of standard retail products are not criminals is not an effective system or control. And assuming that the law doesn't apply to you because you only deal with UK customers flies in the face of existing UK legislation.

The reality is that regulation is getting tighter and stricter. Legislation demands that financial institutions adopt a more sophisticated approach to customer screening in response to mounting criminal activity and complex global terrorism networks. This can only be achieved through accurate, regular, automated screening. It is a logical extension that as our intelligence about criminal activity grows, so should our pro-active response to that knowledge increase.

**Call Now on: 01223 228450**  
**Email: [info@datanomic.com](mailto:info@datanomic.com)**



Datanomic Ltd, 140 Cambridge Science Park, Milton Road, Cambridge CB4 0GF  
T +44 (0)1223 228400 F +44 (0)1223 228401 E [info@datanomic.com](mailto:info@datanomic.com)