The View from the EEMA Chair

The extent of ID fraud was placed under the media spotlight earlier this month, when the UK's fraud prevention service, Cifas, revealed that 2016 witnessed the highest number of identity frauds since records began. Whilst the numbers (172,919 reported incidents) made shocking reading for consumers, it really doesn't begin to scratch the surface in comprehending the vastness of the problem we face.

One of the biggest issues is that a huge amount of ID fraud is not reported, as either it is a low value transaction that goes unnoticed, or that it is unreported for fear of the ramifications from insurance companies (particularly true of businesses). Even when such crime is reported, it is often below the threshold that the police are interested in investigating.

Unfortunately, the cumulative totals across all of the EU can be significant.

We need ID fraud to be well and accurately reported, so that it can be addressed effectively. What is more, there needs to be cross-border perspective as the criminals are to a large extent blind to geography. If a criminal makes 20,000 fraudulent €5 transactions from bank accounts in UK, through mainly automated crime, that is a healthy €100,000 haul. However, scale that across the 28 EU Member States and that is €2,800,000. Not a bad return on investment for very little effort! So, if we are going to make any impact on reducing incidents, it is the responsibility of everyone to report every suspected incident no matter how small – and the authorities to listen. Ideally, I would like to see a well-publicised online portal where victims of ID fraud can quickly and anonymously post details of their theft.

As ID professionals, we have a duty to educate, as well as develop and promote, solutions, strategies and best practice to thwart the would-be ID thief. However, it is also a fact that even today in our

digital-centric lives, a large number of ID thefts have their origins in paper theft, so simple steps such as shredding documents, better password management (NIST recently released new guidelines) and restricting how much digital documentation is printed can be a very effective countermeasure. This applies to consumers as much as commercial organisations.

I would also stress that whilst cases of localised opportunistic ID thefts do occur, there is a far more sinister underbelly, with IDs being stolen and used for international money laundering of cash, which has in all likelihood had its origins in extremely nefarious activities.

When it comes to prosecuting ID theft, there need to be stiff penalties that act as a real deterrent. Much has been made of the fines that organisations can be given for non-compliance with the EU General Data Protection Regulation (GDPR) that comes into force next May - €20 million or 4% of global annual turnover. In the U.S such was the problem with horse theft in the 19th century, that some states made it a hanging offence! Of course, I am not suggesting such extreme measures, but the lawlessness of the digital world does bear resemblance to the Wild West and we need the Sheriffs to take control.

Today, ID theft like so many other cybercriminal activities (most notably the recent surge in ransomware attacks), is a low risk, low cost and high return 'business model' and until the punishment fits the crime there is little incentive to stop.

Chair of EEMA, Jon Shamah