KCS Group Europe

The Imitation Game

06/12/2017

In New York of the 1930s, the Brooklyn Bridge was sold twice a week. Standard going price: $55,000. The seller was one George Parker, an extraordinarily successful conman, who managed to sell the Bridge to dozens of naïve and easily manipulated Americans, in addition to running scams involving several of America's noted landmarks. Sadly, the lessons Parker can teach us are still very much required today.

KCS is seeing a growing number of cases involving identity. Sometimes it is stolen, sometimes it is assumed, but always it is used as a tool of exploitation, directed against victims with a specific goal in mind: to use the *'identity'*, which may be patchy but which appears to be offering a deal too good to turn down, to fraudulently acquire a large amount of money in a short time. There are three ways in which this is done; in order of increasing severity discussed below.

Firstly there is the social media con: impersonating one member of staff to another and requesting transfers or payments to a very particular bank account. This will typically be made possible through a compromised email account, and enough details harvested from social media to add plausibility to the conman. This is the ultimate evolution of the Spanish Prisoner scam from the 1600s which has been most prominent in recent years through the 419 scams. It does not take much effort to clarify whether such communication is genuine – although surprising numbers still fall for it.

The second level is that of identity theft. In this – which typically refers to someone's online identity and 'life' (as quite often these days the two are interchangeable) – the victim's credit cards, social media profiles, accounts and companies are all stolen and abused, with the impression given that the *'victim'* is legitimately behind these new actions and therefore there is nothing wrong. A memorable case of this saw an entire charity hijacked by scammers (who had been paid to disrupt the founding individual's life to the fullest possible extent) who proceeded to divert thousands of dollars in donations to their own accounts. Moreover, his credit cards began to rack up gigantic bills and sensitive health records were released to competitors – all of which was aimed at damaging his reputation and profiting financially.

The third – and potentially most damaging, and the one which concerns us the most today – is the *'long con'*. This will not see the identity of anyone compromised in a strict manner. Rather, the fraudster will assume an identity (real or fake) and use this to specifically target other victims, on the predication that a particular name or manner will open doors and bring better results than simply targeting any one given person for strict identity and pecuniary theft against them.

One recent example on which KCS was instructed bears this out. A reputable financial investment firm in London was approached by a scion of a royal house. His proposal was for an investment of $2m USD in return for an exclusive

(and lucrative) business relationship. He came with a retinue of eight bodyguards, a private limousine, an entire floor of a luxury hotel and credentials (and prior investment) from some of the world's top financial pathfinders. In short, everything appeared to check out. However, this financial firm had been stung before and requested an investigation into the royal's *bona fides*. There would be no harm done in establishing that he was who he claimed.

Unfortunately, investigation confirmed the entire thing to be a serious fraud. The royal member was in fact a fraudster who had created the entire artifice of his entourage, lifestyle and proposals out of cloth. His MO was to take the top-end lifestyle in everything from hotel suites to three-piece suits, run up huge debts and privileges, attempt to gather investment based upon his *'royal'* persona, and then skip town before the bills – and the clients – caught up with him. Indeed, this scam had been successfully pulled at least half a dozen times prior. This time, because the potential victim adopted an attitude of extreme caution, the holes in the fabrication became apparent and the fraudster found no investment or welcome forthcoming.

And yet, the fact that he (and others of his ilk) had been so successful for so long highlights one of the major problems facing businesses today: can you ever be sure of whom you are dealing with? After all, this chap had all the prerequisites as far as image and appearance are involved, and so persuasive was the feeling this put in the minds of previous victims that they had invested significant sums (which to this day remain unrecovered). He seemed the perfect opportunity.

This is the problem. Something that appears *'too good to be true'* almost always is, and yet (in business at least) there seems to be wilful blindness in looking past the issue. Sometimes the artifice will be of such scale and scope it seems impossible not to be real. Sometimes the chance will be considered worth taking despite the astronomical risks involved. Sometimes the deal is wanted desperately, and matters of who and how become temporarily less important.

Let it not be forgotten, a number of Parker's victims got so far as to erect tollbooths and traffic gates on the Brooklyn Bridge, before being hustled away by some very surprised patrolmen. These are not new tactics but they are proving just as efficient today as a hundred years ago. Whenever one comes across a business deal that seems too perfect, or a partner that seems just a little too clean, a degree of healthy scepticism can negate a potential disaster.

And if you don't believe that – well, I have a bridge to sell you.