Psychics, Cages and Scammers – “If it’s a Psychic Network, why do they need my [Bank Account] number?”

(With apologies to Robin Williams)

Contents

Introduction

By now most of us have heard about scams designed to take advantage of vulnerable customers, manipulating them to part with their hard-earned savings. Some of these involve marriage proposals, requests for emergency funds or donations to bogus charities. All of these are collectively referred to as social engineering scams (**"Scams"**).

The real challenge presented by Scams is that its victims are often too embarrassed or ashamed to contact the police or tell their families, once they've realised, they've been hoodwinked. In some European countries, a real effort is being made to try and detect Scams, so that funds can be intercepted, before they are transferred to some account controlled by a criminal gang.

This case study looks at one of these Scams and examines the complex web of associates, counterparties and financial institutes used by it. Over a 10-year period, this Scam defrauded over USD$200 million from almost 1.4 million North American consumers. Further facts suggest that this Scam has been "repurposed" and run in other jurisdictions including Germany, Italy, Denmark, Finland, Austria, Norway, New Zealand and Australia. Most recently, this Scam has appeared in Japan, Vietnam, Philippines and Russia. It's a bit like the game of Whack-a-Mole: when the Scam is shut down in one jurisdiction, it quickly pops up in another.

Psychic Mail Scam

The Scam in this case is known as a direct mail campaign, where letters asking for donations or promoting the sale of goods, are sent en masse to consumers. We often refer these annoying bits of communication as “junk mail”.

These campaigns target consumers most likely to pay up. They are based on mailing lists sourced from companies, who collate data about consumers, their age and particular areas of interest. This is why you might receive junk mail about wine, while your neighbour receives offers on garden products.

In this Scam, consumers received targeted letters allegedly written by a well-known French psychic (“Astrid”), who foretold of terrible future events that would befall a family member or friend. In exchange for a small fee, Astrid would send the consumer a good luck token that she’d personally held or blessed. The fee charged for these trinkets ranged from USD$5 – $50.

Volume Matters

So, how did this Scam manage to defraud so many consumers out of $200 million when the requested payments were so small? The key element of this Scam is volume.

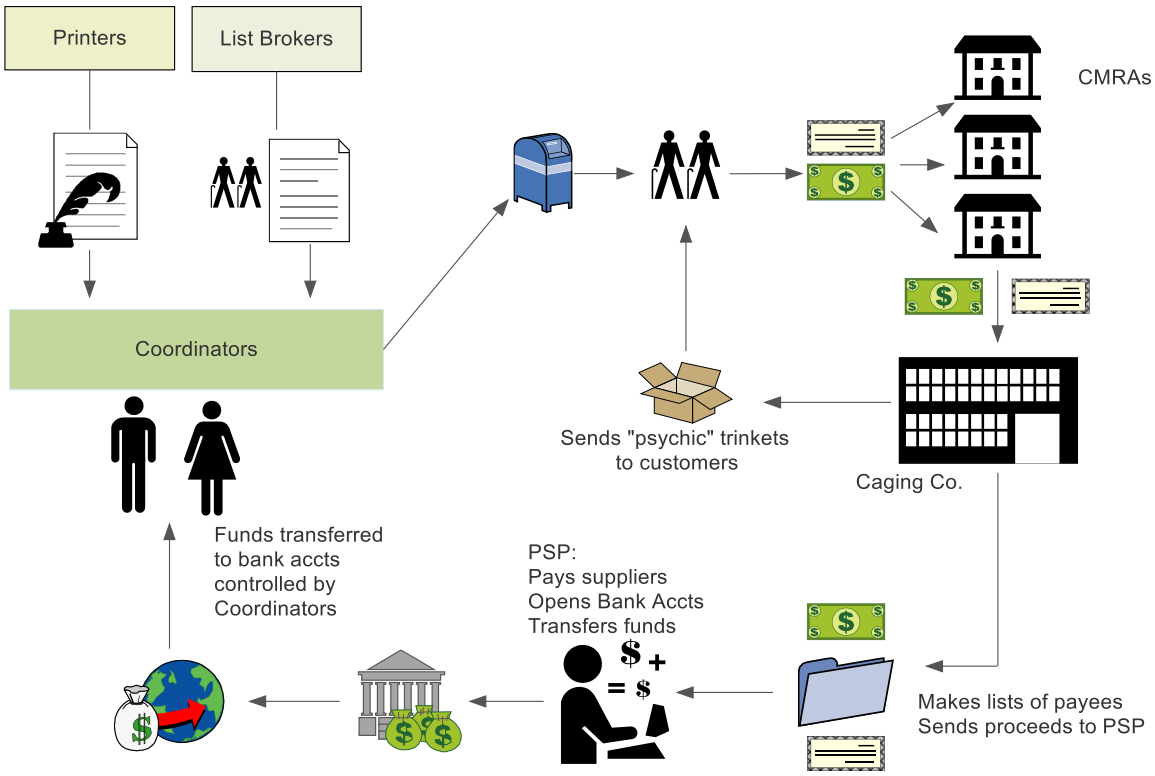
First, the mailing lists obtained by the scammers were so big that, on average, 100,00 – 150,000 solicitation letters were mailed out every month. Each letter included a pre-addressed stamped envelope into which a consumer could send money, cheques and credit card details.

Second, once a consumer responded and sent money, they were immediately placed on a list, where they would then be targeted with more letters from "Astrid" warning of further danger and requiring that more money be sent. Some consumers received as many as 30 to 40 of these back-end letters in a single 6-month mailing cycle.

So, the quantity of mailouts, the small sums involved and encouragement of repeat payments, kept the wheels of this Scam well oiled.

Concealing and Laundering the Proceeds

This case involved what the FATF describes in its 2018 guidance paper as sophisticated money laundering. It required a high degree of organisation and coordination across multiple associates, in different jurisdictions, some of whom had no idea about the criminal nature of the Scam. This diagram is a quick illustration of how the Scam works.



It starts with the individuals who create the content for the mailings, who in this case were the scammers and their associates (**"Coordinators")**, assumed to be located in Europe**.** Once the Coordinators prepared the letters, they were sent to a printer located in Canada, who was engaged to mass produce the mailing material.

Targeted mailing lists were purchased by the scammers from **list brokers**. The letters, once printed, were shipped to the USA and sent out by a **mailing service** to consumers. But, to further muddy the trail of their origin, the Coordinators also arranged for letters to be shipped from Canada to Hong Kong, where associates would then post the letters from there using **commercial carriers**.

Commercial mail receiving agencies (**"CMRAs"**), also known as mail drops, were engaged by the Coordinators to operate private mailboxes where consumers would send their money. The CRMAs were led to think the mail drop was set up for Astrid. This meant that the consumer would use the address of the CMRA on the pre-stamped envelope into which they place their payment, and not the address of the actual scammers.

To muddy the trail further, the Coordinators engaged several different CRMAs to receive the mail, rather than rely on a single provider. This was done deliberately to mitigate the risk of a single CRMA becoming suspicious about the volume of responses Astrid was receiving.

Once the mail was received by a CMRA, it was sent in bulk to a "caging service". These companies open mail, remove the money, make a list of all the consumers who sent money, along with their address details and forward the proceeds to a payment service processor (**"PSP"**). The caging company and its CEO were later prosecuted, after a court concluded they must have known this was a scam, because they were opening and reading the response letters.

The PSP in this Scam was located in Canada (**"CanadaCo"**). The PSP would take a cut of the funds sent to them as payment for their services and then arrange for bank accounts and payment transfers to be made to the Coordinators and their bosses. The PSP was in on the Scam and paid the price for doing so (see below).

Use of Shell Companies ("Shellcos")

In this Scam, Shell Companies were used in two ways:

- To open bank accounts with various banks in order to receive the money paid by consumers;
- To be used as the sender of larger sums held at intermediary accounts to the Scam's leaders allegedly held in UK, Switzerland and Lichtenstein.

The tactics when setting up the Shellcos are familiar: the companies were first given names that seemed to be associated with the psychic services offered ("Star Sign", "Future Mystical Group" and "Future Light Research Centre") and identified Astrid as their ultimate beneficial owner. Given the nature of the business, "psychic services", this seemed to fool both the CMRAs who received the mail and were paid by the Shellcos and the banks who held the account into which the payment processor deposited the proceeds received.

However, some consumers' families started to complain to authorities and media sources started to report about the Scam. Banks noticed the high volume of deposits being made into the Shellco accounts:

> *"It seems that one by one the US banks that [CanadaCo] is using are beginning to complain about the bad press about [Astrid] on Google. Banks are telling [CanadaCo] that they are not comfortable clearing the [Astrid] cheques. [CanadaCo] feels that if the payee name is not changed fairly quickly then there is a good chance that the banks will refuse the cheques as has happened in Canada. The present high volume of US cheques has drawn more of the bank's attention to this matter.*

… The negative press combined with [Astrid's] healthy volumes is affecting our bank relationships and we are concerned about being penalized with higher fees, or worse, termination of service."

[Extract of real email from CanadaCo to Scam Leaders]

Here was the opportunity needed to for the Scam to finally be discovered by the banks. However, CanadaCo, the PSP, wrote to the leaders of the Scam with a solution:

[CanadaCo] feels that if most of the payments are made out to [Shellco] then the banks won't have a problem processing the few that will still be made out to [Astrid] because it will be a significant lower volume].

Astrid's name was no longer used in association with the Scam's bank accounts. New accounts were opened with US banks in the name of the new Shellcos. The Shellcos has much more bland names, with no reference to anything mystical or spiritual. The PSPs were then instructed to deposit consumer payments into these new accounts, instead. Once this change was made, transactions resumed without question and continued to be processed by the banks.

When concerns were later raised by other banks about the volumes of business being processed by CanadaCo, CanadaCo incorporated its own Shellco and used it to open a new account in the UK through which it processed payments for the Scheme. Problem solved.

Screening Blind Spots – Consumer Account Use

Perhaps more problematic was the number of consumers who, victimised by repeated mailings and requests for money, paid large sums of money to the Scam, with no detection or intervention on the part of their banks.

CanadaCo, however, was aware that complaints from family members to the banks could reveal the true nature of the Scam. To mitigate this risk, CanadaCo established a system to stop processing payments if a consumer had already made multiple payments that were likely to raise questions by their family or bank:

> *"The chronic multi-buyer screen is designed not to interfere with enthusiastic responders. Rather, it catches those that can be considered to have a problem - the ones that too often result in a call placed by a son or daughter to an Attorney General. The definition of chronic multi-buyer is an individual that buys the same product more than 60 times within a 90-day period using the exact same bank account or credit card."*
>
> ***[Extract of real email from CanadaCo to Scam Leaders]***

Yes, CanadaCo was advising the Coordinators, using a risk-based approach, that multi-buyer consumers were "high risk". Not for money laundering, but for both the cost vs. benefit of dealing with them and the risk of their families discovering the illegal nature of the Scam.

Current State of Play

To date, several parties involved in the Scam have been prosecuted. CanadaCo was placed on the OFAC sanctions list, along with several of its key executives, who were also criminally prosecuted in Canada.

Investigations also found companies connected to the Scam that were listed on the UK's Companies House registry. Their controllers are allegedly based in Switzerland, yet they are not named as shareholders or directors on the registry. These companies have since been dissolved.

Efforts were being made to extradite one of the Scam leaders, who is thought to reside in Spain, back to the US for prosecution. Another leader is said to have run it from various residences in Canada, Switzerland, the Netherlands, Costa Rica, France and Spain.

A blogger found that websites set up for similar Scams were registered by an individual identified by the US authorities as the Scam's leader who is thought to be in Switzerland.

The investigation into this Scam continues…

Concluding Thoughts

From a CDD perspective, what I find most striking in this case is the risk management tactics used by the scammers and CanadaCo to avoid detection, maintain cash flows and create the illusion of ordinary business activity.

Not only did they think ahead and plot out ways in which to muddy the trail of their mailing activities, they monitored account activity and re-assessed the risks that some types of customers might pose to the Scam's longevity.

They had a clear idea throughout about their risk appetite. When changes could not be made to meet their appetite i.e. opening accounts under different names or banks, they elected not to assume the risk i.e. advising that multi-buyer consumers were not worth pursuing any more. And they were constantly on the look-out for emerging risk areas that could lead to the detection of the Scam.

We talk about undertaking customer due diligence, ongoing KYC and understanding the nature and purpose of the business and its expected activities. But sometimes we forget that criminals are not only familiar with these requirements, but they also apply some of the same practices.

The more serious question this: how was the activity on multi buyer accounts able to go on for so long, allowing the transfer out of so much money, and was not red flagged as being inconsistent with its expected use? How did the KYC held for these retail consumers inform the monitoring of how these accounts were being used?

And perhaps most importantly, how can other forms of CDD – including the use of adverse media – allow for more prompt detection of social engineer scams, where its victims are, unable or too ashamed, to tell anyone about it?

Written by

Samantha Sheen
Financial Crime Advisor

Sam.sheen@efilimited.com

Sam is a financial crime prevention professional with over 15 years of practical experience in compliance. Sam holds a number of qualifications and is recognised as a subject matter expert in the field of financial crime. Sam's previous work experience includes working as MLRO, Data Protection Officer and CCO and Group Head of AML for various financial institutions, both offshore and in Europe.

Sam also worked offshore for several years as the first legal counsel to the financial regulator in Guernsey and subsequently set up the financial crime division, overseeing the examination of a variety of financial institutions. She continues to maintain ongoing engagement with other regulators on financial crime matters. Sam has extensive training experience in the field of financial crime prevention and corporate governance matters. She has most recently been involved in projects related to FenTech businesses, the use of RegTech to mitigate financial crime and list management relating to the screening of customers and third parties. Sam is an ACAMS Alumni who most recently worked with ACAMS Europe as its AML Director. Sam is recognised by ACAMS as a subject matter expert in sanctions and has co-authored a number of online certificate courses. Originally from Montreal, Quebec Canada, Sam holds a Bachelors of Public Administration, Law Degree, qualified as a barrister and solicitor and holds her Masters in Business, specialising in risk management.

Efficient Frontiers International (EFI)

Efficient Frontiers International (EFI) is a Client Focused services organisation, partnering with Financial Institutions to deliver Expertise and Capability and give clients confidence in a complex regulatory and business environment.

Our strategic capabilities cover three principle areas: Consultancy and Advisory, Operations and Technology and Data. This blend of abilities allows us to partner with clients through from insightful advice on emerging regulation, to detailed technical and operational implementation, either as a delivery partner or a managed service provider. Maintaining the regulatory traceability, rigour and client confidence throughout. Our diverse experience has helped us identify critical success factors that all businesses need to focus on, this is what makes EFI a market leading partner.

If you wish to discuss any of the points covered, please do not hesitate to contact us

Russell Taylor
Director of Sales

Russell.taylor@efilimited.com

Rob Windle
Head of Propositions

Rob.windle@efilimited.com
Phone: +44 (0)7811 210 264