The Banker
GLOBAL FINANCIAL INTELLIGENCE SINCE 1926

Catching them while he can: what Frank Abagnale did next

By Jane Cooper | Published: 05 January, 2015 | Comment on this article

Frank Abagnale's story of cheque forger-turned-good guy is well documented in print and on film. His career has seen him work in partnership with 41st Parameter CEO and founder Ori Eisen. They tell Jane Cooper about their work to stay one step ahead of the cyber criminals.

Frank Abagnale thinks digital cheques are a great idea. Especially for people with a criminal mind.

In the US, since the introduction of Check 21 in 2003, recipients of a cheque can make a digital image of it and process that instead of the paper version. It's easy, explains Mr Abagnale: you're selling a house to a cash buyer for $580,000 and you ask them to pay you by cheque, which they write and give to you. You then distract them – by choking and asking them to get you a glass of water – and while they are out of the room you take a photo of the cheque with your smartphone. You send the digital image to your bank to be processed before they come back in the room. Then you say: "I've changed my mind – I don't want to carry this cheque around with me. Why don't you wire it to me instead?" as you tear up the paper cheque. They wire the $580,000 to you, and before they realise it, you have received the payment twice.

Fault checks

When a new banking product is introduced, this is the kind of scenario that Mr Abagnale would dream up to pick holes in the original design. And if banks are smart, they will run their latest ideas past Mr Abagnale before they release them to the public. "Technology breeds crime. It always has and it always will," says Mr Abagnale.

He believes however, that digital cheques – even though they are becoming more ubiquitous – will not fully replace the physical cheque. Large companies, he says, like the float they get from holding onto the money for a bit longer while a physical cheque clears. Of the predictions for a paperless society in the US, Mr Abagnale says: "You will see a paperless society when you see the paperless toilet."

Mr Abagnale does warn, however, that cheque fraud is much easier now than it was 40 years ago. Back then, when he was a teenager, to fraudulently produce cheques he had to rent a six-metre long Heidelberg printing machine, and learn how to operate it himself even though it usually needed three operators. Such exploits were portrayed in the movie 'Catch Me If You Can', where Mr Abagnale was played by Leonardo DiCaprio. He would invent the company's bank account and the signatory that would appear on the fake cheque.

"Today I can open up my laptop, look up the company building, capture their logo, design a cheque in 15 minutes, go to the office supply store, and put it into an inkjet printer," he says. To find the bank account number is just a matter of calling the accounts receivables department – "they will tell you" – and a signature can easily be found in the annual report, he adds.

On the side of the law

Not that Mr Abagnale makes a living doing this kind of thing anymore. These days he is a poacher-turned-gamekeeper who has been working as a consultant – to the Federal Bureau of Investigation, among others – for the past 38 years.

One of the firms he advises is 41st Parameter, which was founded by Ori Eisen in 2004, and was acquired by data analytics firm Experian in October 2013. Mr Abagnale explains that he met Mr Eisen when he was in charge of fraud prevention at American Express, when he encouraged him to leave and set up his own technology company. Mr Eisen would not do it without the support of Mr Abagnale and today they are a good-cop, bad-cop double act in finding the best way to prevent fraud. Mr Eisen comes up with a solution, Mr Abagnale picks holes in it, which they liken to playing a game of chess.

"Data analytics is the best tool in the world to fight crime," says Mr Abagnale. One method 41st Parameter uses is to track the in-built time stamp on devices to detect whether transactions are fraudulent. If someone is attempting to buy something from a mobile, the solution asks the device 'what time is it?'. At a basic level, if the device says it is 6:08 and it is 3:08 in the UK, where the customer is, that could be a signal that a fraudster in Russia, and not the true customer, is trying to make the purchase.

One of the most insidious types of fraud, says Mr Eisen, is "replay attacks" where a criminal can capture someone's security credentials by intercepting a transaction and then replaying that information at a later date for a fraudulent transaction. By using the time-detection method of the device, 41st Parameter's solution will detect that the time is from a past date. In one case that Mr Eisen and Mr Abagnale are familiar with, a bank customer – who had access to a large treasury account – was the victim of a replay attack, and had it not been detected a transfer of $90m would have been paid into the wrong hands.

An inconvenient hurdle

Mr Eisen says there are three elements that are important in transacting online: security, convenience and privacy. "Ever since the internet became popular convenience has been the most important," he says, adding that with each innovation that comes along, fraud becomes easier for the criminals. "At one point we will hit a wall – the losses [companies] incur will be more than the cost of running a business. The convenience factor will have to stop unless there is a new method of security," says Mr Eisen. Typically in a bank, he adds, it is the marketing and sales teams that are asked about an innovation first, "and they ask the risk guy last what they should do".

Security problems have hit the US cards industry hard in a number of data breaches of late, where attackers got inside the network of retailers and infected point-of-sale systems with malware to capture cardholder data. US retailer Home Depot was involved in a high-profile breach in September 2014 in which the data on 56 million cards was compromised. A few months later, in November 2014, the company added that 53 million email addresses had also been compromised in the malware attack. Earlier, in January 2014, retail company Target raised its previous estimate of the number of cards that were compromised in its 2013 cyber attack to 70 million.

Mr Abagnale points to a problem whereby consumers have been conditioned to think that this is not their problem because they do not bear the liability for any fraudulent transactions. What is more worrying, says Mr Abagnale, is the other data that retailers hold on their customers. Say, for example, they have bought a refrigerator and have also applied for finance at the till – this way the retailer is holding other information such as date of birth. And buying a subscription to a credit monitoring service – to detect spikes in activity on your accounts – is useless, says Mr Abagnale. "One year [of credit monitoring] is worthless – you need to buy more than three years' worth," he says.

Customers may only concern themselves with people stealing their credit card numbers to make purchases in the near future, but that is not the main issue. What happens in more than three years' time is more of a concern: cyber criminals are gradually building up a complete picture of an individual's private data, which can be used to launch a much bigger, more sophisticated attack on them at a later date.

Closer to home, Mr Abagnale was himself a victim of a cyber attack at his regional tax office. The South Carolina State of Revenue suffered a breach, which meant that Mr Abagnale's complete tax return, containing sensitive information, along with the digital image of his cheque, was stolen. "Every breach, of course, is because someone inside the company did something they were not supposed to do," he says. In this case, it was at least one staff member opening an email that infected their computer with malware, giving the hackers access to passwords to log into the tax office's network.

On hearing this news, Mr Abagnale would have been forgiven for thinking that digital cheques are not such a great idea, especially for the victims of cyber crime.