Meet Resistant AI, making digital interactions safer from attack

As part of our quick fire questions series – or QFQs – we spoke to Martin Rehak, CEO and Founder of Resistant AI about digitally enabled financial crime, using state-of-the-art AI to beat cybercriminals, and why now is the time to start your company.

We set up the company in 2019; this is our second venture after we built Cognitive Security a few years earlier, a business that was later acquired by Cisco. Since then, we have seen that cybercrime and financial crime have converged. With our background in successfully using machine learning to combat cybercrime involving vast quantities of data and attacks conducted at high speed, we felt uniquely placed to deal with this problem.

At least 80% of financial crime is now digitally enabled, or “cyber”. Whilst the threat to networks and the overall security of businesses remains, cyber criminals are just as focused now on extracting financial benefit from their attacks or using financial systems to move money around that has been generated by other predicate crimes, such as fraud, drugs, and other schemes.

To do this, they are using skills imported from other cybercrimes to circumvent the automated – and often vulnerable – processes that companies rely upon to conduct business online. Thus, we see a blurring of the lines between fraud, money laundering, and cybercrime.

Financial crime actors are highly organised, well-resourced, and extremely innovative. They leverage some of the same “fintech” technology as their targets and have access to significant computing power as well as vast datasets sourced from identity theft. These tools are then brought to bear at a very large scale and at a speed that businesses struggle to deal with. When they are not engaged directly in financial crimes, the criminals are often to be found offering their services to other like-minded individuals, enabling others’ crimes via fraud-as-a-service, full-feature toolkits for enabling fraud.

Tell me about the business – what it is, what it aims to achieve, who you work with, how you reach customers, and so on?

Resistant AI is all about making our customers’ digital interactions with their consumers safer from attack. Generally, we aim to make those businesses’ existing platforms and services better, rather than inviting a wholesale replacement. This is achieved by adding AI to those processes, to extract more efficiently from them and make the interactions that they control much safer.

Our services have two main areas of focus. The first is document forgery detection. Our technology can identify evidence of manipulation or forgery in different types of documents, both ID and non-ID, used in a wide variety of B2C and B2B digital interactions. Documents such as pay slips, invoices or bills, passports, ID cards, proofs of age and address, and many more, are at risk of being presented fraudulently. We can quickly and very efficiently sift the good from the bad, speeding up the interaction where documents are genuine and halting them when they are suspicious.

The second main proposition is centred on enhancing anti-money laundering platforms. In the past, criminals had to hire actual people to go to a bank, open an account, receive a sum of money, take it out in cash and then deposit it at another bank. These days, they can do it in seconds via automation and thanks to digital banking. There are many ways a criminal can leverage global banking infrastructure to quickly move illicit funds and obfuscate their origin.

It is generally accepted that systems to uncover the evidence of laundering are inefficient when dealing with “traditional” money laundering and hopelessly inefficient when facing novel, technologically empowered threats. This is what we address by applying AI to make review of transactions simpler and more efficient, as well as automating the evidencing of missed laundering patterns.

We work globally with banks, neo-banks, fintechs, insurers, payment firms, crypto businesses, ecommerce businesses, and others besides. We have found so far that our propositions resonate particularly well with smaller financial institutions who are on a growth trajectory – and looking for more automation in their decisions, rather than taking on more headcount. Businesses' predisposition to using AI can also be a factor. Some businesses are more avantgarde in this respect than others, though overall adoption of AI is really picking up.

How has the business evolved since its launch? When was this?

Resistant AI launched in 2019, but the team has actually worked together for 15 years or so. When we first started in network security, everyone told us we were crazy – that no one would ever use AI to stop criminals. But we sold our former cybersecurity company, Cognitive Security, to Cisco in 2013, and continue to make developments in the field. Now our latest iteration, Resistant AI, continues the fight against cyber and financial crimes.

Due to the nature of what we do, our evolution is based on what our opposition – the attackers – are doing. As soon as we see them evolving new techniques, we need to add another layer of defence. As an example, that's how we ended up with the capability to determine machine-faked documents – we realised it was becoming an increasingly common issue and managed to come up with a relevant system about a year ago.

How are you funded?

Our seed round of funding took place in April 2021 and we raised $2.75M of capital from Credo Ventures and Index Ventures – led by partner Jan Hammer, one of the most prestigious investors in fintech. October 2021 saw our Series A round, which was led by GV (Google Ventures), with participation from our existing investors Index Ventures, Credo Ventures, and Seedcamp and also several angel investors specialising in financial technology and security. This round raised $16.6M.

What has your biggest challenge been so far and how have you overcome this?

The rapid expansion and automation of financial services to minimise friction for customers has created new challenges with regard to verification and risk

management policies and practices. Evaluating if a digital interaction is authentic now depends on referencing a huge amount of data from multiple sources – everything from geolocation and session behaviours to data from merchants, bureaus, and customer profiles. That data needs to be converted into actionable insight in a matter of seconds to allow precise decisions to be made in real time.

Added to which, today's financial fraudsters are becoming experts at targeting these complex digital environments and are using innovations such as blockchain and instant payments to increase the effectiveness and efficiency of their attacks against fintechs, banks and their customers.

How does Resistant AI answer an un-met need?

Highly scalable, invisible, and efficient attacks on businesses' automated processes are on the rise. And so are the technologically empowered attacks targeting them. Despite this, some companies are still using slow, human-driven processes to defend against financial crime. Such processes can rarely deal with the sheer volume of criminal activity and do not scale well for businesses that need to grow.

If you're taking a significant amount of time to do something when your opponent is committing a crime in a matter of seconds, you have basically lost the battle before it even started. We're using our own state-of-the-art AI and machine learning to beat cybercriminals at their own game, in real time, and with technology that scales, learns from past behaviours, and can spot emerging financial crime patterns before it is too late to act on them.

What's in store for the future?

What's next for us is scaling our business. More companies are needing our solutions and we foresee an even bigger demand in the near future due to an expected increase in financial crime.

The role of AI and machine learning is clear, it is the only effective and scalable technique for the data-driven, real-time supervision of modern financial systems. It brings together state-of-the-art document and customer behaviour evaluation to uncover synthetic identities, account takeover attempts, money laundering and other emerging types of fraud plaguing financial services, with much of it having cybercrime origins.

Using a system of continuously refined relationships between the algorithms,

methods and capabilities, data is used to learn behavioural patterns associated with attacks, meaning threats can be mitigated. At the same time, it must be noted that the criminals themselves are also using AI and ML to support their activities, so it is a cat and mouse scenario that financial services must constantly evolve to win.

Today's AI-powered real-time identity forensics solutions can detect advanced financial crime, fraud, and manipulation, and are adept at joining the dots to uncover previously unidentified vulnerabilities in the underlying systems they protect, so that future exploitation can be deterred.

What one piece of advice would you give other founders or future founders?

Now is the time to start your company. The world looks very dark and bleak right now, but that's the best time to go for it.

We launched our first startup in 2009, at the peak of the financial crisis, and I'm so glad we did. There was no one in Silicon Valley, things were cheaper, there were plenty of smart people on the job market, and customers were shopping around. We took advantage of all of that, and future founders should do the same right now.

Martin Rehak is CEO and Founder of *Resistant AI.*

Article by MARTIN REHAK