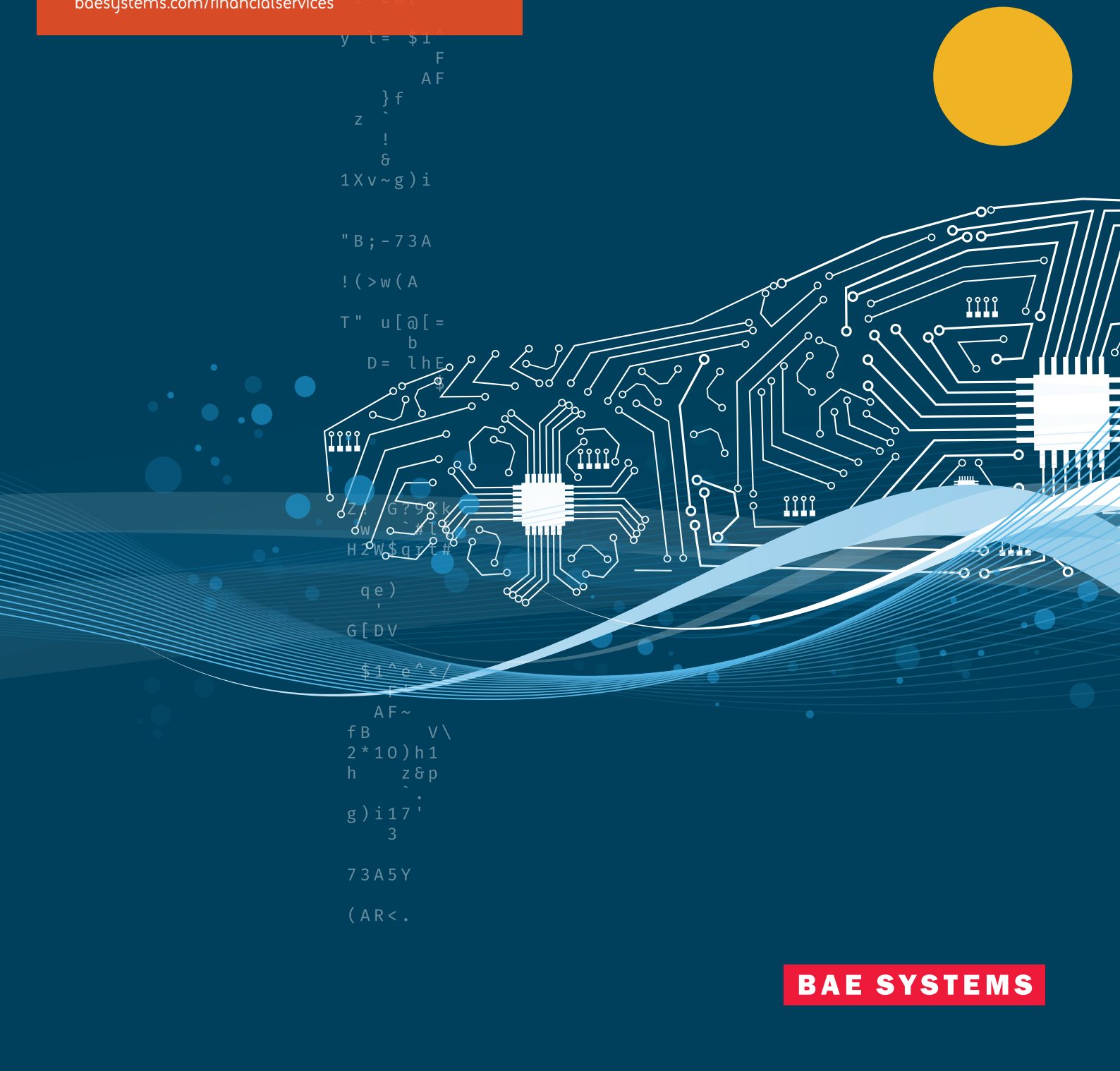
How machine learning can help to uncover car loan fraud and money laundering.

Cleaning up the "Car Wash"

baesystems.com/financialservices



BAE SYSTEMS

Fraud traditionally rises during times of financial crisis and COVID-19 appears to be no different. Some 77% of certified fraud examiners claimed to have seen an increase in recent months, and even more (92%) expect to see it rise further over the coming 12 months.[i] Car financing loans are an increasingly popular choice for fraudsters looking for easy ways to make and launder money. But many financial institutions are struggling to adapt their strategy to tackle an agile foe with the know-how to change tack when new fraud rules are introduced.

An attractive target

Aside from luxury jewellery or property, automobiles are likely to be among the biggest purchases a consumer makes in their lifetime. That makes them an attractive target for fraudsters looking to scam lenders into providing them with loans and then selling the car to launder the profits. One vendor claimed that fraud risk in this space has climbed 38% over the past seven years and reached $7 billion last year in the US alone.[ii]

There are various techniques at the fraudsters' disposal. The dark web is awash with stolen identity data, which could be bought and used to file fake applications. Another option is to create synthetic identities using real and fake data, which are even harder for banks to spot. Sometimes mules may be drafted in, either wittingly or unwittingly, to apply for the car financing loan on behalf of the fraudsters. Or a dealership itself may be in on the scam.

This all presents a challenge for banks keen to minimise fraud losses in a COVID-19 world where cost pressures and business uncertainty have soared in recent months. There are also strict anti-money laundering (AML) regulations at a European and global level which financial institutions must proactively ensure they're in compliance with.

Focus on the data

One such banking customer came to BAE Systems recently after having struggled to stop car financing fraud. The team was applying basic detection rules formulated by in-house experts, but acknowledged that these were difficult to maintain and fine-tune as the fraudsters themselves began adapting their efforts to fly under the radar. They also struggled with both false positives (alerting on non-fraudulent examples) and false negatives (failing to alert on fraudulent examples).

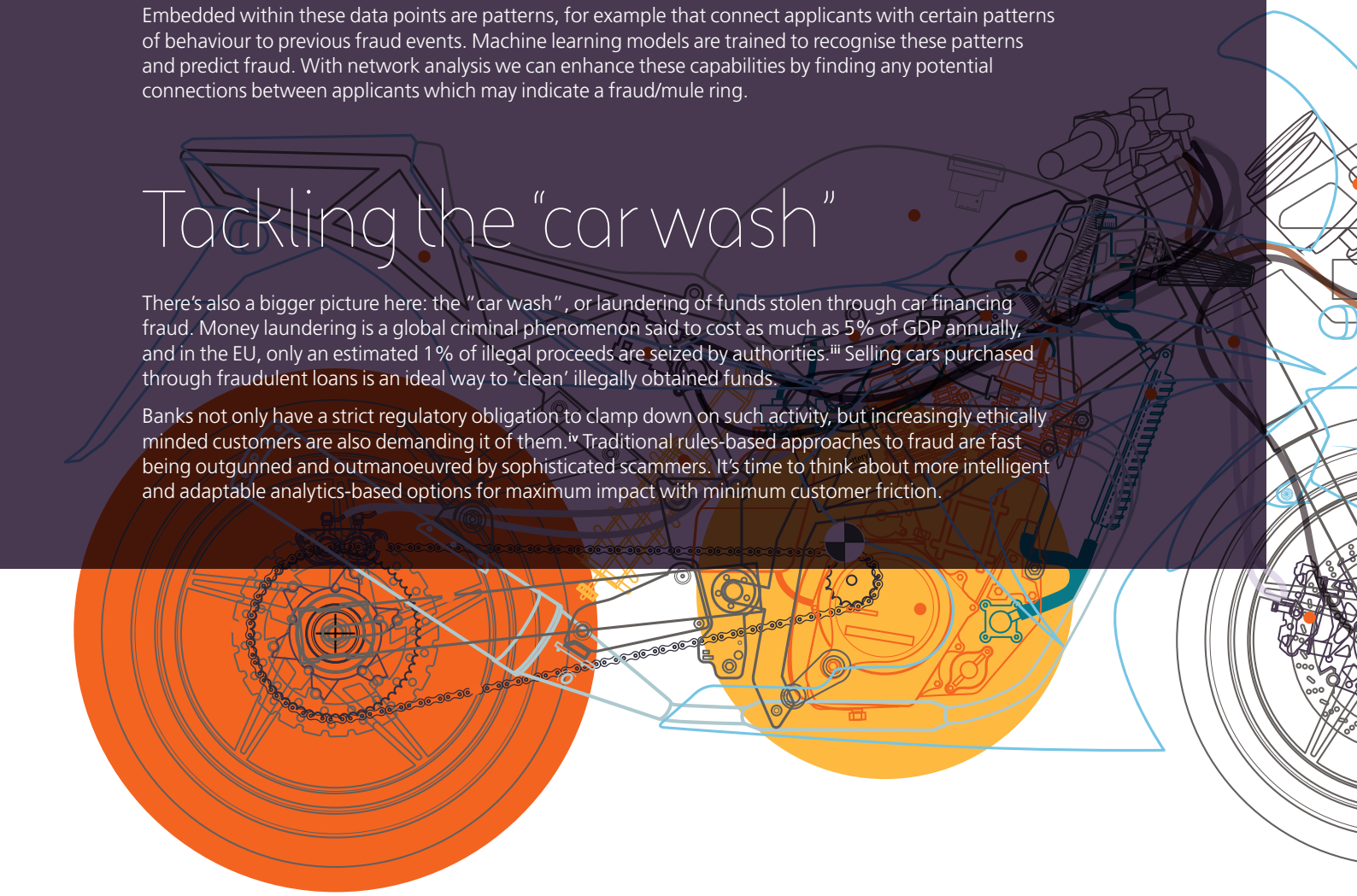
By applying our machine learning algorithms and network analysis techniques, we were able to generate a 360-degree view of each applicant. There were many data points to investigate across these applications, from loan amount and type of vehicle to applicant salary and dealership information.

Embedded within these data points are patterns, for example that connect applicants with certain patterns of behaviour to previous fraud events. Machine learning models are trained to recognise these patterns and predict fraud. With network analysis we can enhance these capabilities by finding any potential connections between applicants which may indicate a fraud/mule ring.

Tackling the "car wash"

There's also a bigger picture here: the "car wash", or laundering of funds stolen through car financing fraud. Money laundering is a global criminal phenomenon said to cost as much as 5% of GDP annually, and in the EU, only an estimated 1% of illegal proceeds are seized by authorities.[iii] Selling cars purchased through fraudulent loans is an ideal way to 'clean' illegally obtained funds.

Banks not only have a strict regulatory obligation to clamp down on such activity, but increasingly ethically minded customers are also demanding it of them.[iv] Traditional rules-based approaches to fraud are fast being outgunned and outmanoeuvred by sophisticated scammers. It's time to think about more intelligent and adaptable analytics-based options for maximum impact with minimum customer friction.



[i] Fraud in the Wake of COVID-19: Benchmarking Report, ACFE (accessed 27 October 2020)

[ii] Auto Lenders Meet to Tackle Rising Fraud Trends at PointPredictive Fraud Consortium Roundtable BusinessWire (June 11 2019)

[iii] The world's dirty money by the numbers, Arnau Busquets Guardi, Politico (May 21 2020)

[iv] The global state of anti-money laundering, BAE Systems, (accessed 27 October 2020)

Author:

David Nicholson, Analytic Product Manager, BAE Systems Applied Intelligence

David is Analytics Product Manager within Financial Services at BAE Systems Applied Intelligence. His work includes setting the strategy and vision for the analytics product, enabling financial institutions to improve detection effectiveness and efficiency through the application of advanced analytics, in particular optimisation, machine learning, and artificial intelligence. David is also a hands-on senior data scientist with over 15 years' experience developing data science solutions in the areas of financial crime, telco, cyber, defence & security. His work has resulted in several publications and international patents.

We are

BAE SYSTEMS

At BAE Systems, we provide some of the world's most advanced technology defence, aerospace and security solutions.

We employ a skilled workforce of 82,500 people in over 40 countries. Working with customers and local partners, our products and services deliver military capability, protect people and national security, and keep critical information and infrastructure secure.

Global Headquarters
BAE Systems
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems
8000 Towers Crescent Drive
13th Floor
Vienna, VA 22182
USA
T: +1 720 696 9830

BAE Systems
19, Boulevard Malesherbes
75008 Paris
France
T: +33 (0) 1 55 27 37 37

BAE Systems
Mainzer Landstrasse 50
60325 Frankfurt am Main
Germany
T: +49 (0) 69 244 330 040

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/5G

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai