



SYNECTICS
SOLUTIONS

FRAUD IS NOW THE MOST COMMON CRIME IN THE UK, WITH FRAUDSTERS WORKING TOGETHER TO OPERATE SUCCESSFULLY. COULD COLLABORATION ENABLE ORGANISATIONS TO FIGHT BACK AND GAIN THE UPPER HAND IN THE FIGHT AGAINST FRAUD?

According to the Office of National Statistics there were 5.8 million fraud and computer misuse crimes in 2017, making them the most common crimes in the UK. Sophisticated technology is enabling criminals to steal and sell data globally, and to commit fraud in high volumes.

Research has shown that the criminals collaborate via restricted user groups and dark web groups, sharing fraud methods, identifying weaknesses in target businesses, and developing new ways to commit their crimes.

This presents a massive challenge for law enforcement and industries like finance and insurance as we seek to prevent and detect fraud - whilst also providing the high standards of service required to meet ever more demanding customer needs.

Could sector-wide collaboration be the solution? In depth research indicates that it is an essential weapon in the fight against fraud.



5.8 million fraud and computer misuse crimes in 2017

Globally each year, **fraud is costing an estimated;**

£3.24 trillion

a sum equal to the combined GDP of the UK and Italy.



The total cost of fraud has been accurately measured across expenditure **totalling;**

£15.6 trillion



Since 2008, there has been a **startling 49.5%** **increase in average losses** with businesses losing an **average of 6.8%** of total expenditure.



The latest research from national audit, tax and advisory firm Crowe Clark Whitehill, together with the University of Portsmouth's Centre for Counter Fraud Studies (CCFS), has revealed **a national fraud pandemic in Britain, totalling £110bn a year.**

Source: The Financial Cost of Fraud 2018. University of Portsmouth's Centre for Counter Fraud Studies.

The Challenge

The dark web has no search engines and is an unregulated wild-west version of the internet. A place where stolen bank details, weapons, drugs, pornography and just about anything can be bought and sold. Global law enforcement monitors the sites and periodically close them down, make arrests and disrupt the criminals. The downside is that within a few months, new sites spring up and the whole process starts again.

The level of sophistication matches many of the best online retailer sites, with user names, ratings and recommendations - even technical support desks and chatbots to help purchasers easily use the illegal data they have bought.

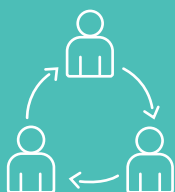
Increasingly, stolen data can be found on the regular web too – the one we all use – sold through closed user groups and even the blatant use of social media.

The fraudsters are bold and seemingly fearless. To combat them, we need to understand how they operate across both the dark web and the regular internet.

Understanding how the fraudsters work

In 2017, fraud detection and cyber security specialists Peter Taylor Consultants commenced a project to research organised fraud and cybercrime, with the main body of research completed in Summer 2018. This paper is based on their findings.

This project consisted of 4 areas:



Meetings and exchanges with cyber security and counter fraud professionals across insurance, banking, online retail and law firms.



Analysis of the fraudsters' training manuals to identify behaviour patterns which are identifiable via technology.



Research on the dark web and restricted sites together with meetings and interviews with selected reformed fraudsters and cyber criminals.



A peer review of our findings with other counter fraud professionals and reformed fraudsters.

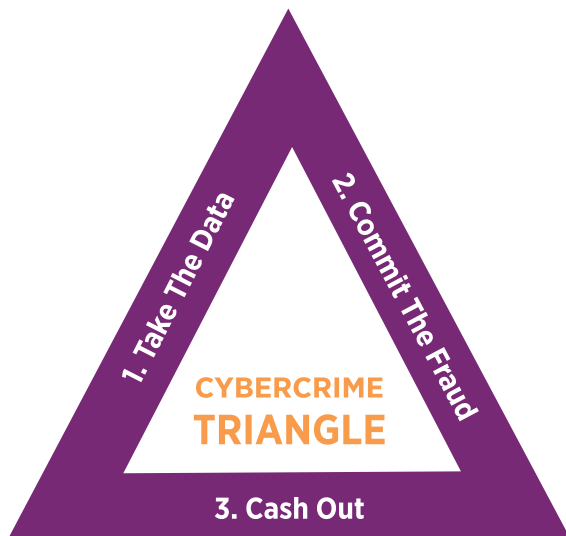
2019: The Cybercrime Triangle

Fraudsters are becoming increasingly audacious. They're worrying less and less about getting caught, as they overwhelm the capacity of law enforcement and fraud teams.

But contrary to popular opinion the most prolific criminals do not steal data, commit fraud and then take the cash. Instead they specialise in crime as a service and the activity they are good at. They are highly dependent on co-operation and collaboration.

Recent court cases have shown that many organised crime gangs and particularly those involved in drugs run with very similar structures to the corporate world. There is usually a CEO equivalent, a board of leaders, operations, and a sales force. Money then feeds back to the top.

The Cybercrime Triangle consists of 3 distinct roles:



1. Obtaining the data needed to commit fraud – e.g. the criminal hackers, social engineers, and corrupt employees or data handlers accessing personal data, email accounts, passwords etc.

2. Committing the fraud – e.g. the fraudster who takes over accounts, open lines of fraudulent credit, ghost brokers, false claimants.

3. Cashing out – e.g. laundering the money through mules, gaming, bogus e-commerce businesses, and dubious investments

"People do what they are good at and get others to help with the things they aren't good at. Most can do one or two of stealing data, committing fraud or cashing out, very few can do all three successfully".

Brett Johnson, reformed fraud gang leader, 2018.

Why This Weakens Efforts to Counter Fraud

- When law enforcement and other authorities combine to close-down well known dark web sites it often only takes only 3-5 months for them to set up again.
- Website and systems owners and cyber security providers work continuously to better protect their data from unlawful access and accidental disclosure – but while this disrupts the fraudsters they can soon switch to new suppliers and use data they hold for other types of fraud. For example, someone who does account takeovers may also use that information for tax refund fraud.
- Fraudsters who 'cash out' tend to have a backlog of resources for money they are laundering – for instance, UK based fraudster Grant West who at the time of his arrest had £1.7m in his Bitcoin account and details of 63,000 debit and credit cards.

The Solution?

Looking at the Cybercrime Triangle, it is apparent that there are weaknesses in the way fraud is currently dealt with, and that there are opportunities which come from understanding the 'enemy' and making it harder for them to operate.

1

Opportunity One

Despite the sophisticated methods outlined above, many frauds are committed successfully by criminals whose devices are visible, whose phone numbers are visible and who use the same email addresses across different frauds in different names. Companies must therefore make better use of how they hold their data and how it is analysed to identify anomalies across different transactions. This needs to be used across all three areas of cybercrime and fraud.

2

Opportunity Two

We need to attack fraud. If there is an attempt to complete a false claim or transaction with a bogus identity and the device, phone or email fails the fraud checks that is currently seen as a success. But that success is limited because those devices and details will continue to be used elsewhere if the information is not shared.

Companies need to collaborate to leave markers across the finance, insurance, online retail and social housing industries for phone, device or email addresses commonly used by fraudsters.

3

Opportunity Three

Many developments are being worked on to improve verification of identities and who businesses are actually dealing with. A while ago the dominant question for businesses was what do we know about this person to decide whether to undertake this risk? Now the dominant question is – is this a real person or a synthetic online identity created to meet the criteria set to meet risk scores?

We are now involved in an arms race with the fraudsters where we try and distinguish between what they do and what genuine customers do.

Collaboration & data sharing

Collaboration is the only way organisations seeking to counter fraud can compete on a level playing field with the organised criminals.

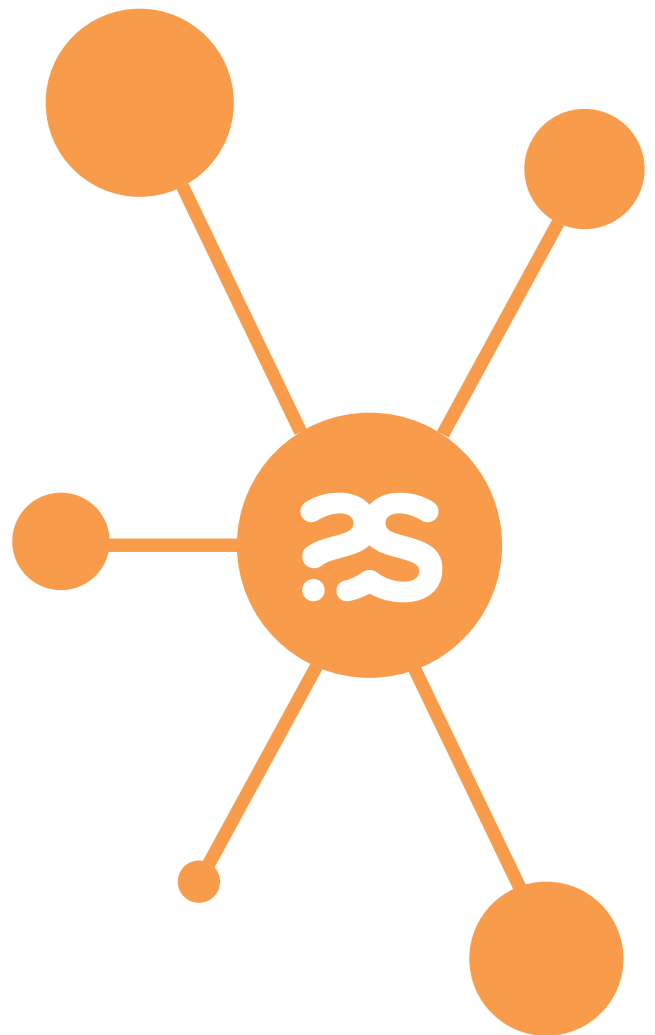
For instance...if a criminal has been blocked from committing a fraud on ABC Bank in most cases, they can target DEF Bank. However, this would not be the case if both these and other banks all shared data about their devices and the details they are using. Once the device and details have been detected the fraud can be stopped by all those sharing the data – banks, online retailers, insurers, social housing and others.

Our research showed that there is huge improvement in accurate fraud detection where data is kept in a way it can easily be shared, and where analytics are in place.


Fraudsters operate wherever there is a route to money and a potential victim. They share tips with each other and tell each other when a fraud works well and who the easiest targets are. They're not short of money to invest in research and technology and of course they operate outside of any laws or regulations.

We must therefore remove the silos and insular thinking that stifles the fight against fraud. As we continue to find newer and better ways to detect fraud, we must share them - ensuring the foundations of collaboration are in place to fully benefit from improvements made by organisations and fraud detection specialists.

This must be through data sharing not just within targeted industries, but also across all channels and across the public and private sectors. Why? Because that is what the fraudsters do, and why fraud continues to grow.



“

**£44
billion** 

The Financial Cost of Fraud 2018 report estimates that the UK economy could be boosted by £44 billion annually if organisations step up efforts to tackle fraud and error.

”

Synectics Solutions and Data Collaboration

Future business success is increasingly being defined by a company's ability to observe and profile behaviour from the data created or consumed by people.

The ability to share and blend disparate data sources in order to create new insight can have a truly transformative effect on organisations' ability to compete.

Synectics Solutions are one of the leading data collaboration companies in the UK, with over 27 years' experience creating, hosting and managing a variety of large data collaboration programmes that have helped to prevent billions of pounds being lost to fraud and financial crime.

With a truly unique body of expertise to draw from we are well positioned to navigate the obstacles to successful collaboration, so clients can easily pick their way through the regulation, legality and other challenges to successfully get their data collection and collaboration services off the ground.



National SIRA and the National Fraud Initiative: Harnessing the Power of Collaboration.

National SIRA, from Synectics Solutions, harnesses the power of collaboration bringing together data from 130+ financial organisations which is further enhanced by third party sources.

Synectics Solutions also works with the UK Government's Cabinet Office and the National Fraud Initiative (NFI) is a large data solution which brings together data from 1300 public and private sector bodies including local authorities and public sector organisations.

This collaborative approach creates a powerful and comprehensive fraud detection and prevention database. National SIRA and NFI provide an outstanding opportunity for organisations looking to be part of a dedicated and collaborative syndicate committed to fighting crime.



For more information about Synectics Solutions, National SIRA, the NFI and fighting fraud through the power of collaboration, please call 01782 664 000 email info@synectics-solutions.com or visit www.synectics-solutions.com

About Synectics Solutions

For over 27 years, we have been providing leading edge data driven solutions to help organisations harness the power of data.

The systems we build and host for our clients are highly successful in creating more profitable customer relationships, reducing risk, combating financial crime, and enabling organisations to meet their compliance and regulatory commitments.

We work closely with our clients to create innovative solutions that meet their data driven challenges. We are renowned in the markets in which we operate for our dedication to customer satisfaction and for providing highly tailored solutions that meet our clients' complex needs.



SYNECTICS
SOLUTIONS

Synectics Solutions Ltd, Synectics House, The Brampton, Newcastle-under-Lyme, Staffordshire, ST5 0QY

0333 234 3418

info@synectics-solutions.com

www.synectics-solutions.com