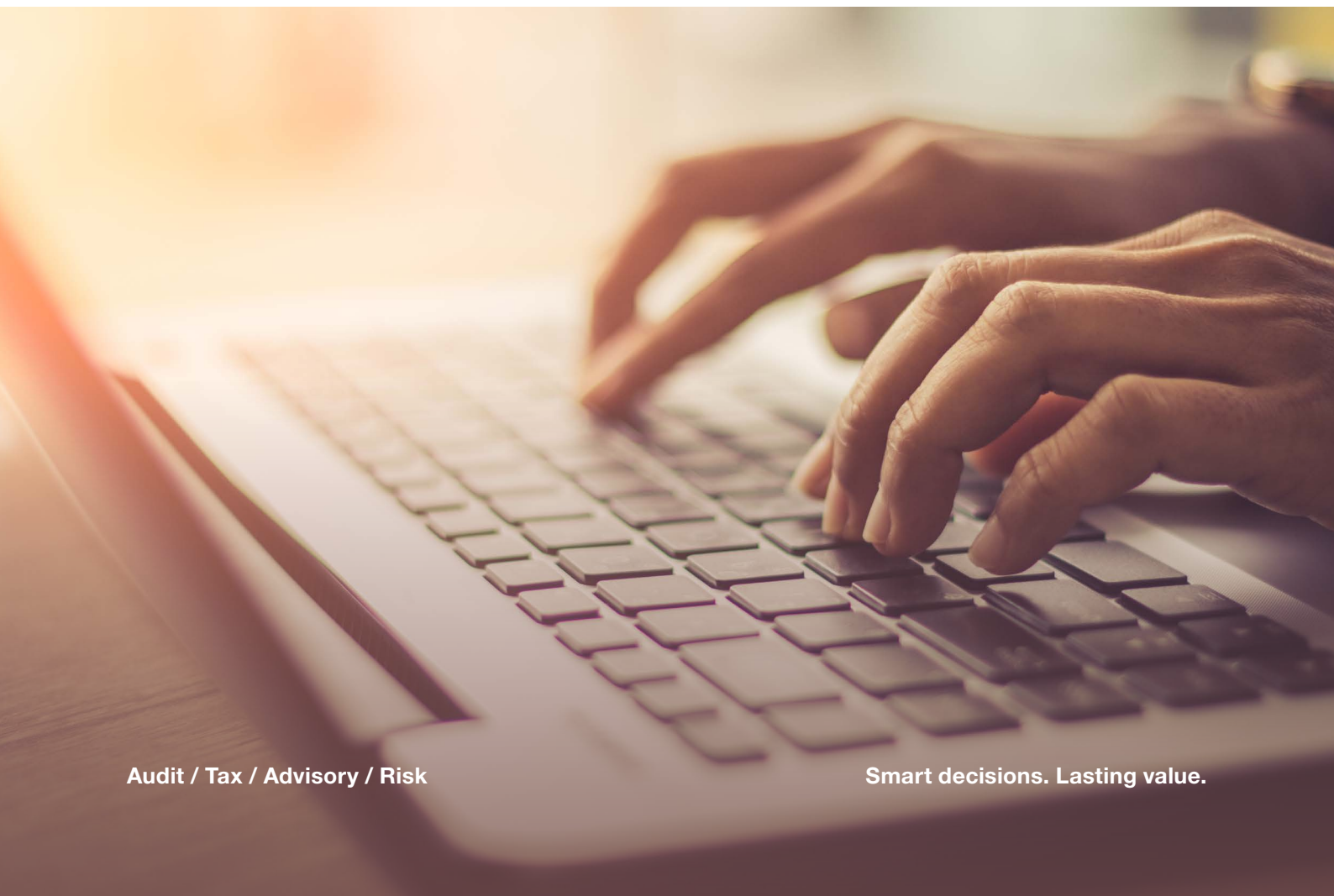


# The Dark Web

## Bad for business

Research into the planning and monetisation of fraud and cybercrime against organisations on the Dark Web

Jim Gee, Lawrie Hall, Dr Victoria Wang,  
Professor Mark Button and Ephrems Joseph





---

# Contents

<b>Introduction</b>	<b>2</b>
<b>What did we find?</b>	<b>6</b>
Banking and finance	6
Telecommunications	10
Retail and entertainment	12
Energy and transport	16
<b>Conclusions</b>	<b>18</b>
<b>How Crowe's Dark Web service can help</b>	<b>19</b>
<b>About the authors</b>	<b>20</b>
<b>About the organisations</b>	<b>23</b>
<b>Appendices</b>	<b>26</b>

## Introduction

This report summarises research into the nature and extent of discussions on the Dark Web with the intent to attack and damage companies through fraud and cybercrime. Monetising those attacks is also often part of the plan.

**Jim Gee**

Partner, National Head of Forensic Services  
Crowe UK

Crowe, in collaboration with the Centre for Counter Fraud Studies at University of Portsmouth and Cyfor, undertook research to find out more about how the Dark Web is used by fraudsters and cybercriminals to support, plan, execute and monetise attacks on companies.

### What is the Dark Web?

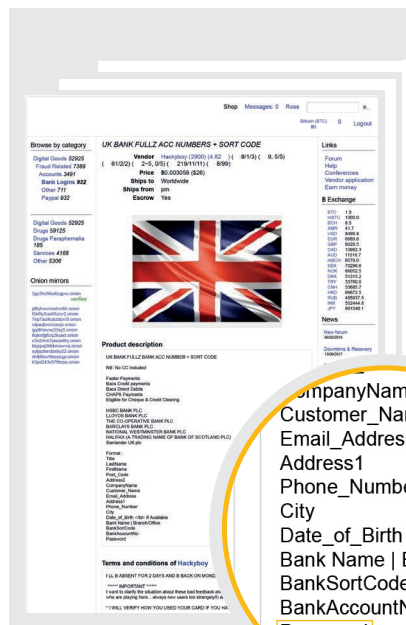
The Dark Web is the World Wide Web content (a series of 'darknets') that requires specific software, configurations or authorisation to access. It forms a small part of the deep web, the part of the Web not indexed by web search engines.

The darknets which constitute the Dark Web include small, peer-to-peer networks, as well as large, popular networks like Tor, Freenet, I2P and Riffle operated by public organisations and individuals.

### Why is the Dark Web bad for business?

The Dark Web is well known for being a marketplace for illegal goods such as drugs and weapons. However, the research underpinning this report originated from a desire to know more about how it is used by fraudsters and cybercriminals to support, plan, execute and monetise attacks on companies.

Little has been published in this area, and yet, as was found during the course of the research, a very real problem exists. It is easy to access and increasingly becoming the source of tools and methods used by criminals to target organisations.



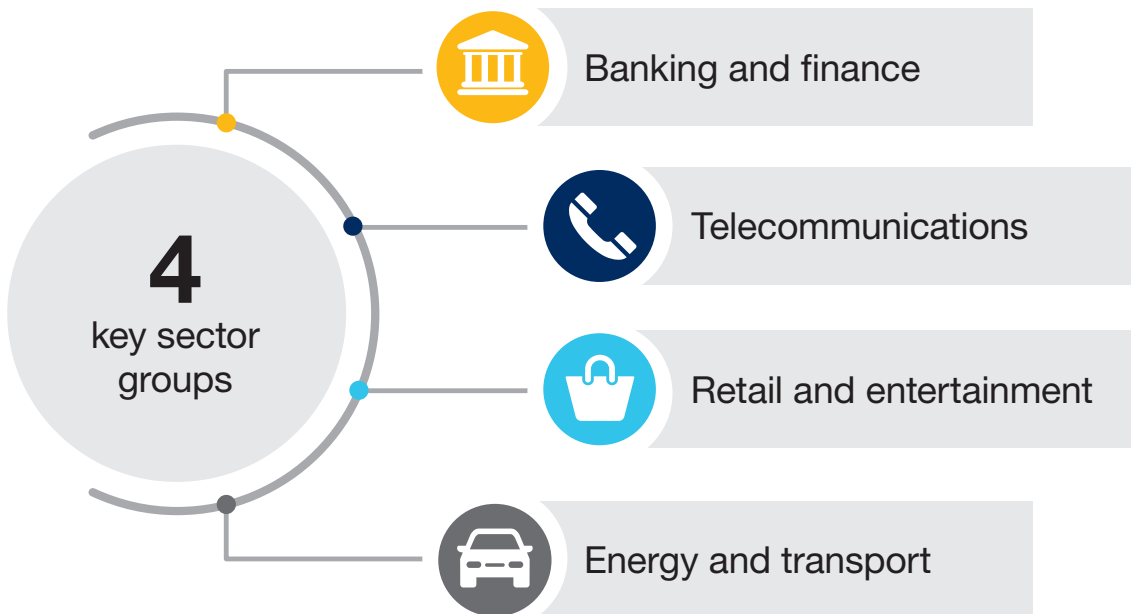
The screenshot to the left is just one example of a listing we found showing carding (read more about carding on page seven). Sensitive personal data like this is easy to access, readily available and cheap to purchase.


**What were we looking for and what did we find?**

The Dark Web is large and complex. To provide a starting point the researchers selected the 50 most valuable UK brands and searched areas of the Dark Web called 'Market Places' for information about each brand.

The researchers quickly found discussions, and attempts to market services and products, intended to defraud or perpetrate cybercrime against 21 of the top 50 UK brands, as identified in the 2017 brand directory league table. The researchers also identified discussions about a large number of other well-known brands.

For ease of analysis, we have split our findings against the top 50 UK brands into four key sector groups.



A person wearing a dark hoodie is seen from the side, sitting at a desk in a dimly lit room. They are looking at two computer monitors. The left monitor displays a complex network diagram with orange and blue nodes. The right monitor shows a web interface with a red box containing the text "Exploitation, Remote Shell" and "Current Log". The person's hands are on a keyboard. The overall atmosphere is dark and focused.

“The researchers quickly found discussions, and attempts to market services and products, intended to defraud or perpetrate cybercrime against 21 of the top 50 UK brands.”

---

## What did we find?

### Banking and finance

Out of the top 50 UK brands, we found eight banking and finance organisations that were affected.

#### What was for sale?

Our research found fraudsters selling fraud packs, template bank statements, utility bills and passports, UK bank account numbers and sort codes, template company cheques, and providing advice on phishing.

#### How is it bad for business?

The fraud tools identified during the research could be used to commit identity theft against individuals and defraud legitimate businesses.





### Sale of 'fraud packs' with access to stolen personal data

'Fraud packs' were advertised for sale, which are bundles of information and guidance to help people perpetrate fraud. Multiple packs were identified for sale that could be used for 'carding' and 'card not present' (CNP) fraud.

Carding is a deceptive process which involves stealing, reselling, and ultimately using large volumes of payment information to commit fraud<sup>1</sup>.

CNP fraud includes transactions that occur over the telephone, Internet or by mail-order where the cardholder does not physically present the card to a merchant<sup>2</sup>.

Carding and CNP fraud is increasing globally. In the UK it was the source of £290.5 million in losses during 2007 and by 2016 had risen to £423.3 million. While the upward trend may reflect the increasing popularity of online shopping rather than an absolute rise in the proportion of carding and CNP fraud, the fact is that the cost is increasing and someone has to pay.



In the UK, CNP fraud was the source of **£290.5 million in losses** during 2007 and by 2016 had **risen to £423.3 million**.

The liability for fraudulent CNP transactions is typically placed on the business selling the fraudulently obtained goods and services. The payment processor, such as Mastercard or Visa, is entitled to claim the entire value of a fraudulent purchase from the business and is exempt from liability. Much like the cost of shoplifting from physical stores, the cost is then passed back to consumers in the form of higher prices.

Personal details used by fraudsters to undertake carding and CNP fraud, such as name and address, can be used for a variety of criminal enterprises. In the worst case scenarios, identity theft linked fraud can result in individual consumers being pursued for bad debts and/or experiencing difficulty accessing credit.

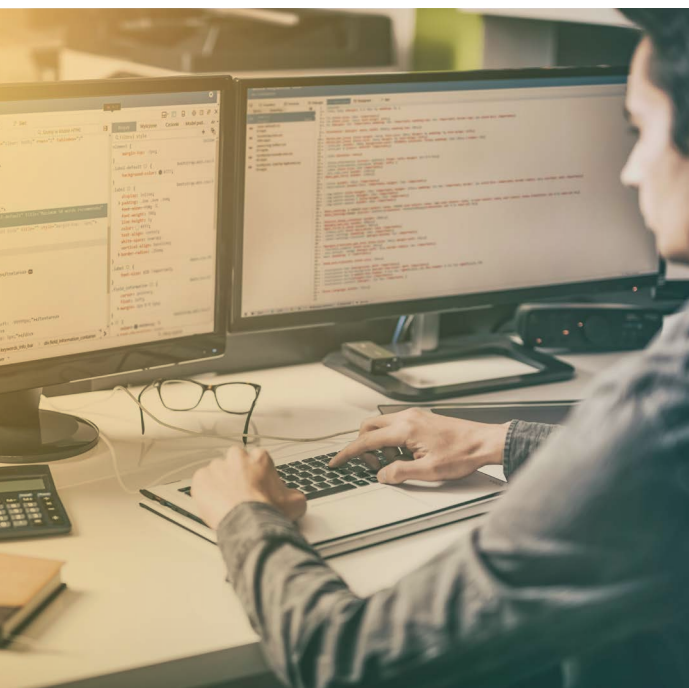
<sup>1</sup> Peretti, K. 2008. Data breaches: What the underground world of carding reveals. Santa Clara Computer and High Tech. L.J., 25, 375–413.

<sup>2</sup> <https://www.uspaymentsforum.org/wp-content/uploads/2017/03/CNP-Fraud-Around-the-World-WP-FINAL-Mar-2017.pdf>

### **‘How to’ guides for phishing**

Phishing is when fraudsters ‘fish’ for potential victims through a variety of mediums, such as emails or phone calls, to obtain personal details for fraudulent purposes<sup>3</sup>.

Phishing has been around for at least 25 years<sup>4</sup> and continues to pose a major threat to organisations. Fraudsters often employ phishing techniques to trick organisations and individuals to unlawfully redirect payments and transfers to bank accounts accessible to the criminal.



Phishing-related losses can be substantial. Invoice fraud causes approximately £9 billion in losses to UK SMEs each year<sup>5</sup>, with 25% of SMEs having experienced a fraudster attempting to redirect cash transfers. Individuals can lose their entire life savings.

### **Template bank statements**

Bank statements are often required by organisations as proof of identity, address and income and expenditure. Editable template bank statements are used by fraudsters for a variety of purposes including, for example, identity theft, concealment of bank transfers and direct debits, benefit fraud, fraudulently obtaining goods on credit, and individuals taking out loans they are not entitled to.

Template bank statements can also be used to obtain other identification documents, such as a driver’s licence, which creates additional opportunities to commit fraud.

3 Action Fraud. N.d. Phishing, vishing and smishing. Retrieved 05/09/2018 from <https://www.actionfraud.police.uk/phishing>

4 James, L. (2005). Phishing exposed. [electronic resource]. Rockland, Mass : Syngress Pub.

5 Business Comparison. 2018. Invoice fraud: are you aware of the dangers to your SME? Retrieved 05/09/2018 from <https://www.businesscomparison.com/blog/invoice-fraud-aware-dangers-sme/>



### **UK bank account numbers and sort codes**

Once bank account numbers and sort codes are obtained by a fraudster there is a high chance the account will be compromised and/or the account details sold to another fraudster.

A 2015 hack of UK telecommunications company TalkTalk affected 157,000 TalkTalk customers, including 16,600 bank account numbers and sort codes. It was subsequently established that individual personal information obtained during the hack was for sale for £1.62 per person<sup>6</sup>. One businessman targeted by fraudsters using the information lost over £20,000.

### **Passport templates**

Passports are a versatile tool in many frauds. They are 'foundation' documents used as identity verification for a host of other services that can be used to build a false identity. For example, a passport may be required when opening a bank account, and the bank statements subsequently used as proof of address. Once a false identity is created it is much easier for fraudsters to operate successfully.

### **Company cheque templates**

Company cheques are used by organisations to pay bills and settle invoices. The use of cheques has declined significantly in recent years, from 40% of worldwide transactions in 2005 to 8% in 2014. It is also likely to have continued to decrease further since 2014. The UK has followed a similar downward trend, with the number of cheque transactions decreasing by 79% in the last 20 years.

Despite the decline in use, cheques are still used by fraudsters. Template company cheques can be used to trick businesses into accepting fraudulent payment for goods, or in some cases fraudsters can even cash false cheques.



**Invoice fraud** causes approximately £9 billion in losses to UK SMEs each year, with 25% of SMEs having experienced a fraudster attempting to redirect cash transfers.

<sup>6</sup> The Mirror. 2015. Hacked TalkTalk information on sale to organized fraud gangs for £1.60 a time. Retrieved 05/09/2018 from <https://www.mirror.co.uk/news/uk-news/hacked-talktalk-information-sale-organised-6744695>

---

## Telecommunications

Out of the top 50 UK brands, we found six telecommunications organisations that were affected.

Out of the top 50 UK brands, we found six telecommunications organisations that were affected:

### **What was for sale?**

Our research found fraudsters selling stolen internet services, methods to steal money from people via ATM machines, and 'free' online TV accounts.

### **How is it bad for business?**

The information identified could be used to commit theft, digital piracy and intellectual property fraud intended to defraud legitimate businesses.

### **Stolen Internet services**

Theft of Internet services involves unlawfully obtaining access to Internet services by physically rerouting internet cables or hacking into a wireless router. In the most extreme cases, hackers have decoded encryption used by telecommunication providers to create illegal set top boxes that provide access to digital TV channels.

Stolen Internet services reduce the income of telecommunication companies, and could also provide a means to compromise the security of online activity undertaken by individuals and organisations.

### Stealing money via ATMs

'Mobile cash out' is a service provided by some banks that enables customers to withdraw money from an automated teller machine (ATM) without the use of a debit card. Instead of a debit card, a code is sent to an individual's mobile phone and the code can be used to withdraw money from the ATM.

Fraudsters have quickly learned how to manipulate the process, often employing phishing techniques to obtain personal information from unsuspecting bank customers. The information is then used by the fraudster to obtain the codes necessary to withdraw cash without a debit card.



78.5 billion visits to pirated film and TV content websites in 2015.

### 'Free' online TV accounts

Online TV accounts, such as Netflix, are a popular way to access TV shows and films. Our research identified fraudsters on the Dark Web selling 'lifetime' access to various online TV subscription services, including cable sports channels, for less than \$10. As this type of fraud becomes more common its impact will be increasingly significant.



There were 78.5 billion visits to pirated film and TV content websites in 2015, and almost 30% of Britons admitted to watching illegal movies online or buying counterfeit DVDs in 2014, a figure that is likely to be substantially higher in 2018. The cost to UK audiovisual companies is around £500 million a year, and emerging evidence suggests that sports fans are moving away from paying for sports packages and streaming individual games instead. Sky's early-season ratings dropped by a fifth in 2016, with BT's Champions League coverage also struggling<sup>8</sup>.

7 Business Insider. 2016. Illegal streaming is dominating online piracy. Retrieved 05/09/2018 from <http://uk.businessinsider.com/illegal-streaming-is-dominating-online-piracy-2016-8?r=US&IR=T>

8 The Guardian. 2016. 'Even my 78-year-old father streams' – why football fans are switching off. Retrieved 05/09/2018 from <https://www.theguardian.com/football/2016/oct/26/football-fans-stream-sky-bt-sport-live-viewers>

---

## Retail and entertainment

Out of the top 50 UK brands, we found four retail and entertainment organisations that were affected.

### What was for sale?

Our research found fraudsters selling guides to obtaining counterfeit designer goods, shopping receipts with loyalty points, counterfeit shopping vouchers and details for 'cracking' online store accounts.

Furthermore, there was also evidence of fake online accounts with customer reviews, store cards with balances, online subscription accounts and video games.

### How is it bad for business?

The information identified during the research could be used for the sale of counterfeit goods, card cracking and digital piracy.



### Counterfeit designer items

One listing identified contained a counterfeit Burberry watch for sale, which was described as a 'copy' or 'replica' watch in the terms and conditions.

The production and sale of counterfeit designer items has a significant impact on the global economy, costing around half a trillion dollars each year, with American businesses and industries losing approximately \$200 billion in revenues<sup>9</sup>. The rise in counterfeit products can cause corporations to not only lose millions, sometimes billions, in revenue, but it can negatively impact their reputation, and result in an increase in costs<sup>10</sup>.

There are also wider implications, with approximately 2.5 million jobs being lost due to the counterfeit black market. Considering the rising productivity and prevalence of counterfeits, which shows no signs of abating, unemployment<sup>11</sup> should be expected to increase further as a direct result of this illicit activity.

### Shopping receipts with loyalty points

Our research found fraudsters selling supermarket loyalty points on eBay<sup>12</sup> and the Dark Web<sup>13</sup>, which has also been evidenced in recent articles. Typically the points are sold at a substantial discount to their face value. It is not clear how the points are obtained by the fraudsters in this case, however three fraudsters have previously been arrested after spending over £17,000 worth of stolen Tesco Clubcard points.

Most major UK supermarkets offer forms of loyalty schemes for their customers. In exchange for purchasing goods, supermarkets provide customers with points that can be redeemed for goods and services with the retailer, and can also be used with other businesses such as restaurants.



**2.5 million jobs** being lost due to the **counterfeit** black market.

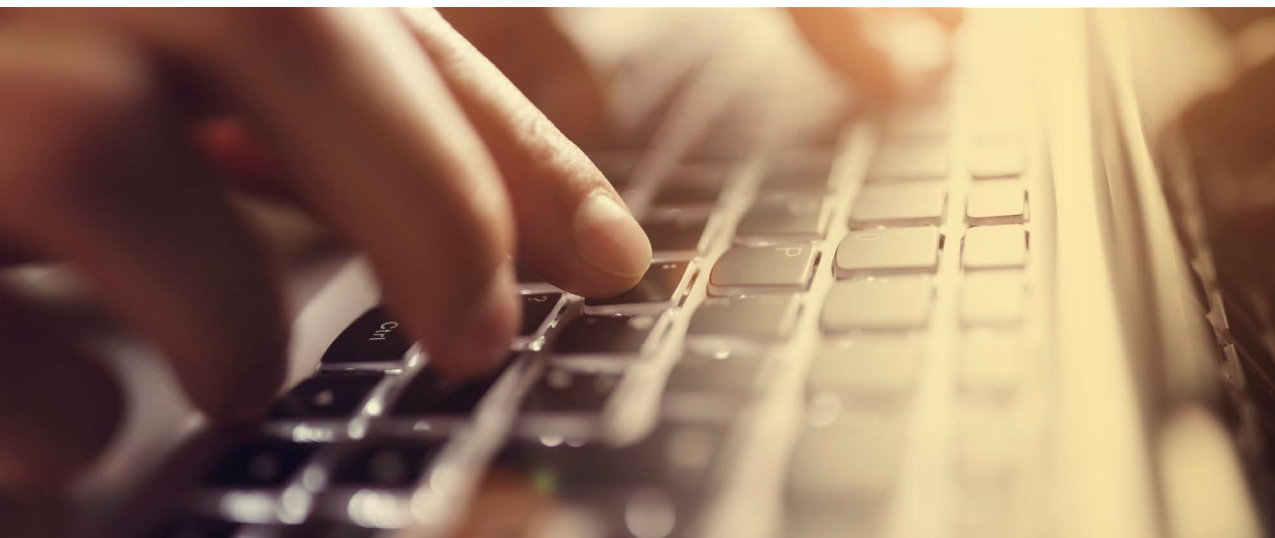
9 Sowder, A. The harmful effects of counterfeit goods. Retrieved 05/09/2018 from <http://www.athens.edu/business-journal/spring-2013/asowder-couterfeit/>

10 Security. 2016. How counterfeits impact sales of genuine products. Retrieved 05/09/2018 from <https://www.securitymagazine.com/articles/87198-how-counterfeits-impact-sales-of-genuine-products>

11 Trade Vigil. 2017. Negative Effects Of Counterfeiting On Brands. Retrieved 05/09/2018 from <https://www.tradevigil.com/negative-effects-counterfeiting-brands/>

12 Money Saving Expert. 2015. Tesco shopper? Beware buying or selling Clubcard vouchers on eBay. Retrieved 05/09/2018 from <https://www.moneysavingexpert.com/news/2015/04/tesco-clubcard-user-beware-buying-or-selling-vouchers/>

13 Telegraph. 2013. Drug dealers using 'dark web' to sell Tesco vouchers. Retrieved 05/09/2018 from <https://www.telegraph.co.uk/news/uknews/crime/10671468/Drug-dealers-using-dark-web-to-sell-Tesco-vouchers.html>



### **Counterfeit shopping vouchers**

Shopping vouchers remain popular and are often given as gifts. We found that fraudsters are offering counterfeit shopping vouchers for sale on the Dark Web. It is likely the vouchers are for use in physical stores rather than online.

### **Details for 'cracking' online store accounts**

One Dark Web listing identified during the research contained detail for cracking online store accounts.

Cracking often features the unauthorised access of an online account through discovering the password by a variety of means. This is usually achieved by recovering the passwords from the data stored, or transporting between, computer systems. The account is 'cracked' when the password is repeatedly guessed by a computer algorithm using numerous combinations until the account is compromised.

Cracking is often used to commit fraud by gaining unauthorised access to a computer without the owner being aware. Personal details are stolen or sold on, such as accessing banking information which could have a significant cost to individuals or businesses.



---

### **Fake online accounts, with customer reviews**

We found a listing of fake online accounts with customer reviews. A fake online account is often created by using false details to open an account on a website. The reviews are often written by individuals or software that have never used the service. Fraud therefore arises through creating a false business to appear trustworthy and creditable, which can be used for fraudulent purposes. Fake reviews can also be used to negatively affect another company's reputation.

### **Store cards with balances for sale**

Our research identified listings with store cards with balances for sale. Cards are often stolen through physical theft, cloning, and the exploitation of programming errors by the merchant<sup>14</sup>. The unlawfully obtained cards are then sold only for a discounted price.



A common method of extorting store cards with funds from organisations is through a data breach, which happened in 2015 to Woolworths in Australia. The company was hacked which led to the leak of AUS \$1.3 million worth of gift cards online<sup>15</sup>.

Starbucks also experienced two types of gift card fraud with a security researcher discovering a flaw in the gift card value-transfer protocol, which could be exploited to allow attackers to move balances between cards without the use of the card. A second incident involved attackers exploiting the auto-load feature on the gift cards that allowed them to rapidly drain any attached bank accounts<sup>16</sup>.

14 LPM Insider. 2018. Gift card cloning. Retrieved 05/09/2018 from <https://losspreventionmedia.com/insider/retail-fraud/gift-card-cloning/>

15 Tripwire. 2015. Gift card fraud: How it's committed and why it's so lucrative. Retrieved 05/09/2018 from <https://www.tripwire.com/state-of-security/risk-based-security-for-executives/risk-management/gift-card-fraud-how-its-committed-and-why-its-so-lucrative/>

16 Infosec Institute. N.d. Gift card fraud: A profitable business. Retrieved 05/09/2018 from <https://resources.infosecinstitute.com/gift-card-frauds-a-profitable-business/#gref>

---

## Energy and transport

Out of the top 50 UK brands, we found three energy and transport organisations that were affected.

### What was for sale?

Our research found fraudsters selling template utility bills from energy providers and air miles from a high profile airline.

### How is it bad for business?

The fraud tools identified during the research could be used to commit identity theft, or to defraud organisations.

### Template utility bills

Similarly to template bank statements, editable template utility bills are used by fraudsters for a variety of purposes such as identity theft. They can be used to obtain other identification documents such as a driver's licence, which can then be used to commit further fraud.



## Air miles for sale

One listing advertised stolen air miles for sale. Fraudsters are hacking the accounts where the points are held and selling them online for a cheaper price.



Russian cybercriminals hacked 30,000 worth of air miles from one couple and used them for a holiday, while over 3,600 customers purchased one seller's fraudulent hotel and car rental services on AlphaBay between March 2015 and December 2017<sup>17</sup>. The amount of fraudulent flights resulted in one US bank blocking all purchases of flights going in and out of the country.



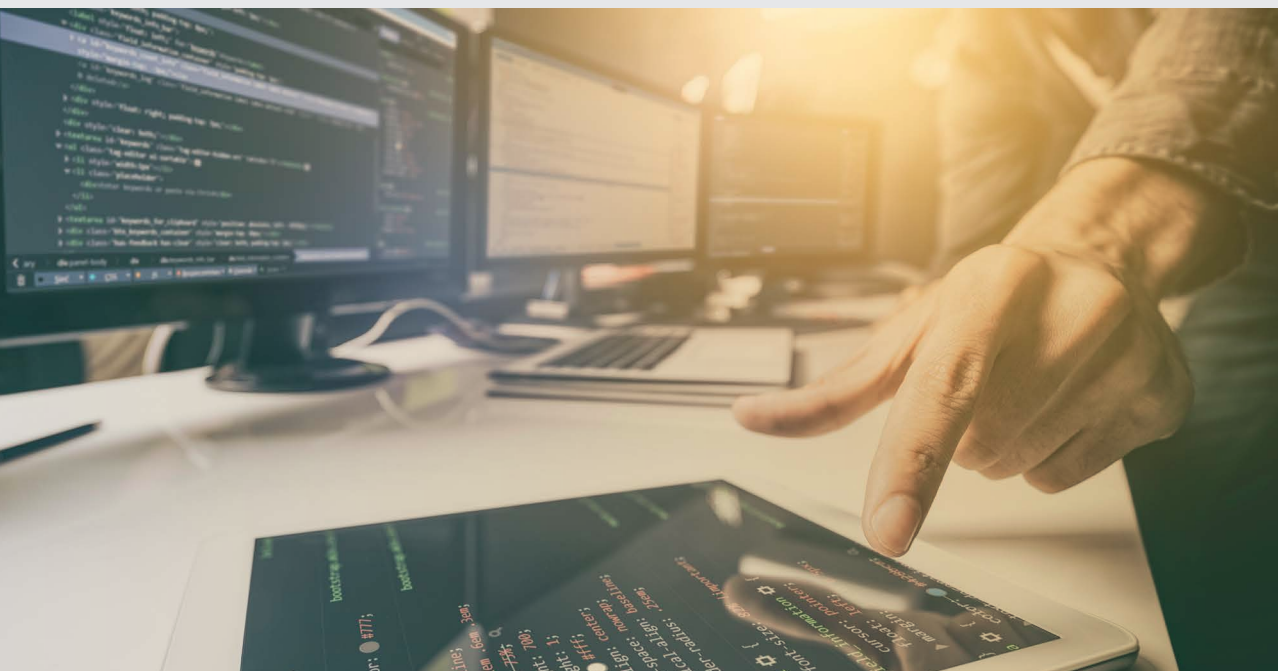
The amount of **fraudulent flights** resulted in one US bank blocking all purchases of flights going in and out of the country.



<sup>17</sup> Independent. 2017. Russian cyber criminals stealing British people's reward points and Airmiles to go on luxury holidays. Retrieved 05/09/2018 from <https://www.independent.co.uk/news/uk/crime/avios-points-stolen-airmiles-cyber-crime-account-russian-luxury-holidays-fraud-flashpoint-research-a8068126.html>

# Conclusions

Our research demonstrates that cyber criminals collaborate and trade online to obtain the information and tools necessary to defraud and commit crime.



This happens on a significant scale with many of the UK's top brands affected. This report, by exposing the nature and scale of what is happening, can help to raise awareness of the problem.

Fraud and cybercrime are now the most commonly reported crime and no organisation can expect to be immune. Businesses can and should do much more. There are mechanisms available to allow more effective threat assessments.

More research is also needed, and the work of the Centre for Counter Fraud Studies and Dr Victoria Wang should be supported and repeated to cast further light on specific sectors where the damage that Dark Web-organised fraud and cybercrime has significant impact.

---

## How Crowe's Dark Web service can help

The Dark Web requires expertise to search it effectively and discreetly. Searching should be undertaken by trained experts who are used to working across the various Dark Web market places.

Crowe offers a low-cost subscription service for organisations interested in monitoring the Dark Web for emerging threats. It can be deployed quickly and provides a regular report of any discussions relevant to the organisation.

Crowe's service is much more than is offered by automated Web 'crawlers'. Searching is undertaken by humans, specially trained with an eye for detail and the intelligence to spot threats and points of interest.

For more information and a no obligation discussion please contact us:

**Jim Gee**

Partner  
Head of Forensic Services

[jim.gee@crowe.co.uk](mailto:jim.gee@crowe.co.uk)  
+44 (0)20 7842 7239

## About the authors

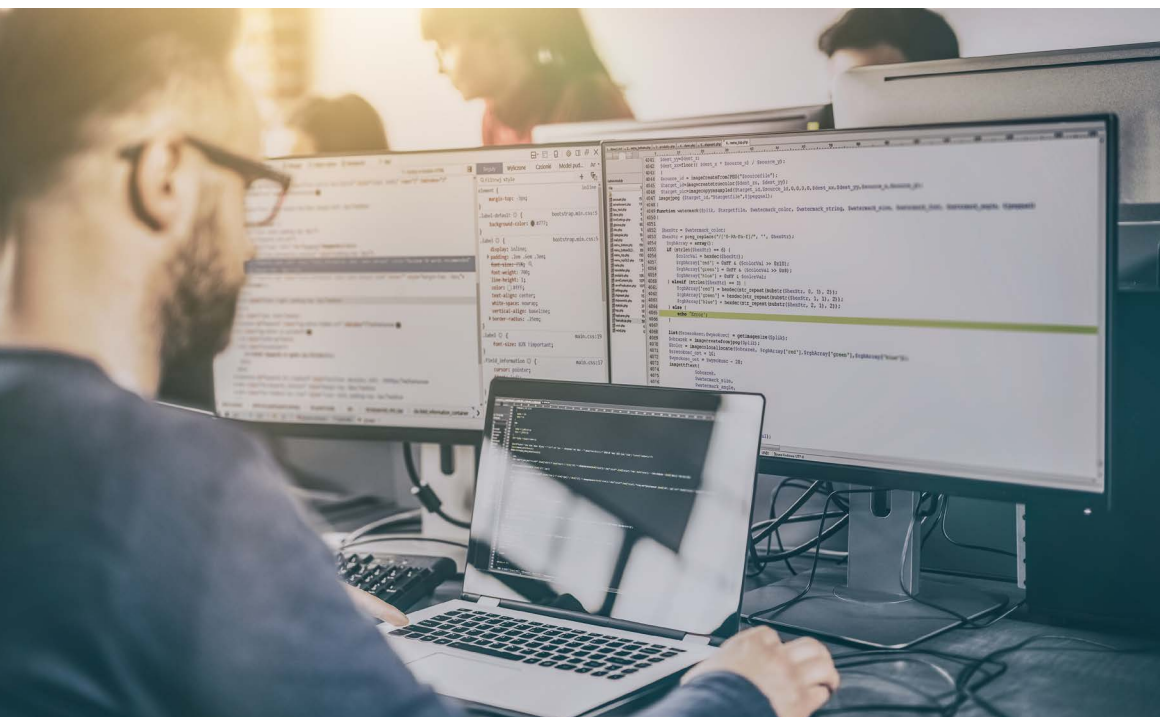


### Jim Gee

Partner, National Head of Forensic Services  
Crowe UK

Jim is a Partner and National Head of Forensic Services at Crowe UK. He is also Visiting Professor at the University of Portsmouth and Chair of the Centre for Counter Fraud Studies (Europe's leading centre for research into fraud and related issues) and Chair of the UK Fraud Costs Measurement Committee (a cross-sector body) which, each year, develops and publishes the UK Annual Fraud Indicator.

During more than 25 years as a forensic specialist, he has advised Ministers, Parliamentary Select Committees and the Attorney-General, as well as national and multi-national companies, major public sector organisations and some of the most prominent charities. To date he has worked with clients from 41 countries.





## Lawrie Hall

Commercial Director  
CYFOR

As a Director, Lawrie leads CYFOR's commercial department with a strategic, consultative and personal approach. Experienced in all disciplines at CYFOR, Lawrie is predominantly responsible for advising clients on the management of digital evidence, including the application of Forensic techniques and eDiscovery technology. Lawrie has successfully integrated data analytics to various projects ensuring the intelligence of the software is

fully utilised. As a qualified Project Manager, Lawrie has provided expert consultancy on a range of high-profile, complex and multi-jurisdictional Forensic Investigations. While at CYFOR, his entrepreneurial and committed approach has seen the business establish new ventures, innovating the Corporate Investigations division and securing the continued growth and development of the company.



## Dr Victoria Wang

Senior Lecturer  
University of Portsmouth

Victoria is a senior lecturer on security and cybercrime at University of Portsmouth. Her current research ranges over cybersecurity, surveillance studies, and general technological developments. Victoria's latest research projects include: i) data release and its related issues of trust, privacy and security; ii) cyber security management measures in organisations;

iii) formal methods for monitoring, data collection and interventions; iv) a general formal theory of digital identity and surveillance; v) the techno-social theory of 'Phatic Technology' as a conceptual tool to understand cyberspace; and vi) cybercrime and threats in various countries, e.g. Nigeria, and various networks, e.g. the Darknet.



## Professor Mark Button

Director of the Centre for Counter Fraud Studies  
University of Portsmouth

---

Mark is Director of the Centre for Counter Fraud Studies at the Institute of Criminal Justice Studies, University of Portsmouth. Mark has written extensively on counter fraud and private policing issues, publishing many articles, chapters and completing eight books with one forthcoming.

Some of Mark's most significant research projects include leading the research on behalf of the National Fraud Authority and ACPO on fraud victims; the Nuffield Foundation on alternatives to criminal prosecution, the Department for International Development on fraud measurement, Acromas (AA and Saga) on 'Cash-for-Crash fraudsters', the Midlands Fraud Forum and Eversheds on 'Sanctioning Fraudsters'.

Mark has acted as a consultant for the United Nations Office on Drugs and Crime and on Civilian Private Security Services. He also holds the position of Head of Secretariat of the Counter Fraud Professional Accreditation Board and he is a former director of the Security Institute. Before joining the University of Portsmouth Mark was a Research Assistant to the Rt. Hon. Bruce George MP specialising in policing, security and home affairs issues. Mark completed his undergraduate studies at the University of Exeter, his Masters at the University of Warwick and his Doctorate at the London School of Economics.



## Ephrems Joseph

Doctoral Student at the Institute of Criminal Justice Studies  
University of Portsmouth

---

Ephrems Joseph is a doctoral student in the Institute of Criminal Justice Studies (ICJS), Faculty of Humanities and Social Sciences at the University of Portsmouth.



---

# About the organisations

## Crowe's Forensic Services

Crowe's Forensic Services are designed to help clients whatever the problem, wherever the place. We help clients to react to an adverse event or to better protect themselves against such events in the future. We have delivered such services across most continents, and in some of the most difficult countries in which to operate.

**We offer a full range of forensic services including:**

- Fraud investigations
- Forensic accounting
- Financial crime
- Cybercrime protection
- Whistleblowing
- Corporate intelligence
- Counter fraud advisory
- Training and mentoring.

Our aim is to deliver significant financial benefits for clients which far exceed our fees.

Crowe's team are specialists with a high-level national and international track record built up over many years. We have advised clients of all different types and sizes, including governments, major national and international companies and high profile charities. Our people hold professional qualifications and have many years of practical experience.

We adopt a business approach to fraud, cyber and forensic issues, making sure your organisation is as financially healthy and stable as possible, for now and the future.

For more on Crowe UK visit:  
[www.crowe.co.uk](http://www.crowe.co.uk)

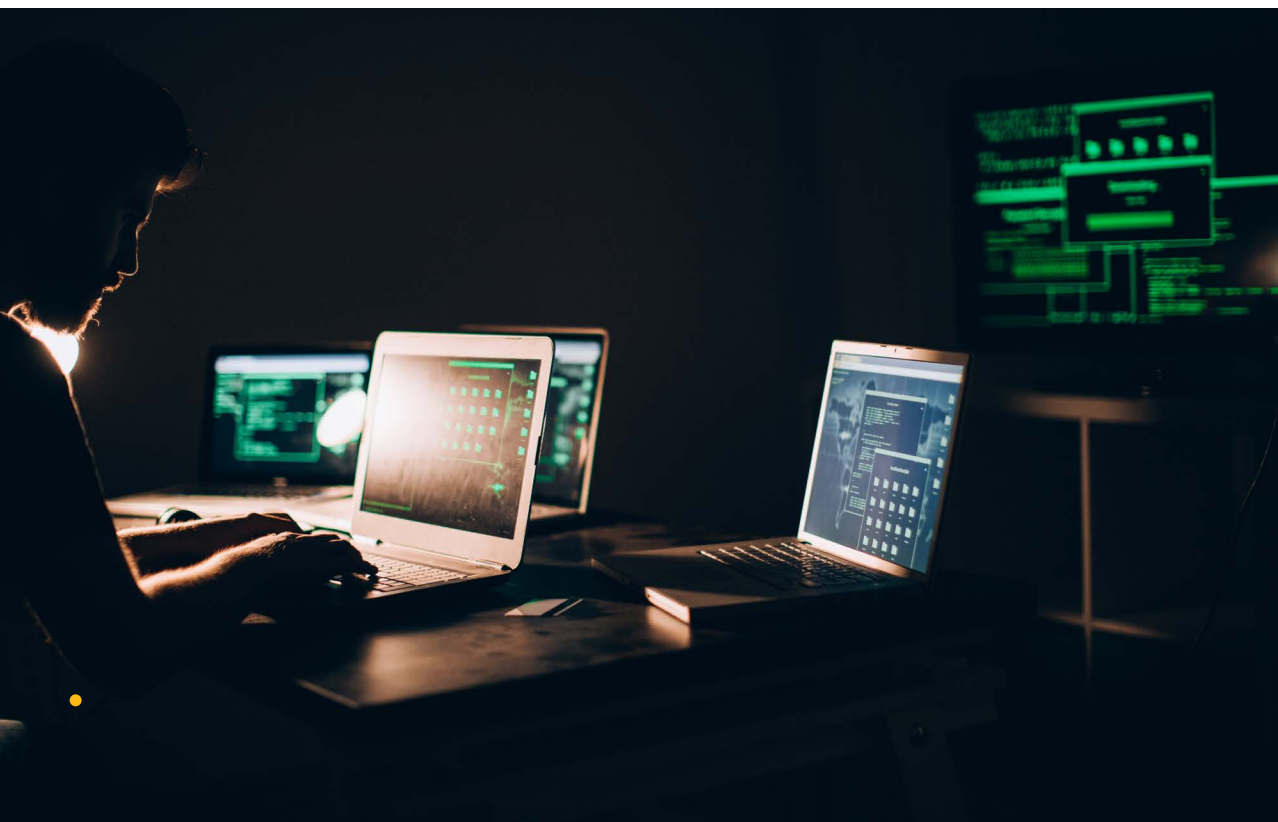
## Centre for Counter Fraud Studies (CCFS)

The Centre for Counter Fraud Studies (CCFS) is a specialist research centre at the University of Portsmouth.

CCFS formed in 2009 to accommodate the growing interest in counter fraud that has occurred over the last 10 years. The Centre aims to collate and present the widest possible range of information regarding fraud and the solutions applied to it, and to undertake and publish further research where needed. Additionally, the Centre's Fraud and Corruption Hub

gathers the latest thinking, publications, news and research in one central resource for counter fraud professionals.

For more about CCFS visit:  
[www.port.ac.uk/centre-for-counter-fraud-studies](http://www.port.ac.uk/centre-for-counter-fraud-studies)



---

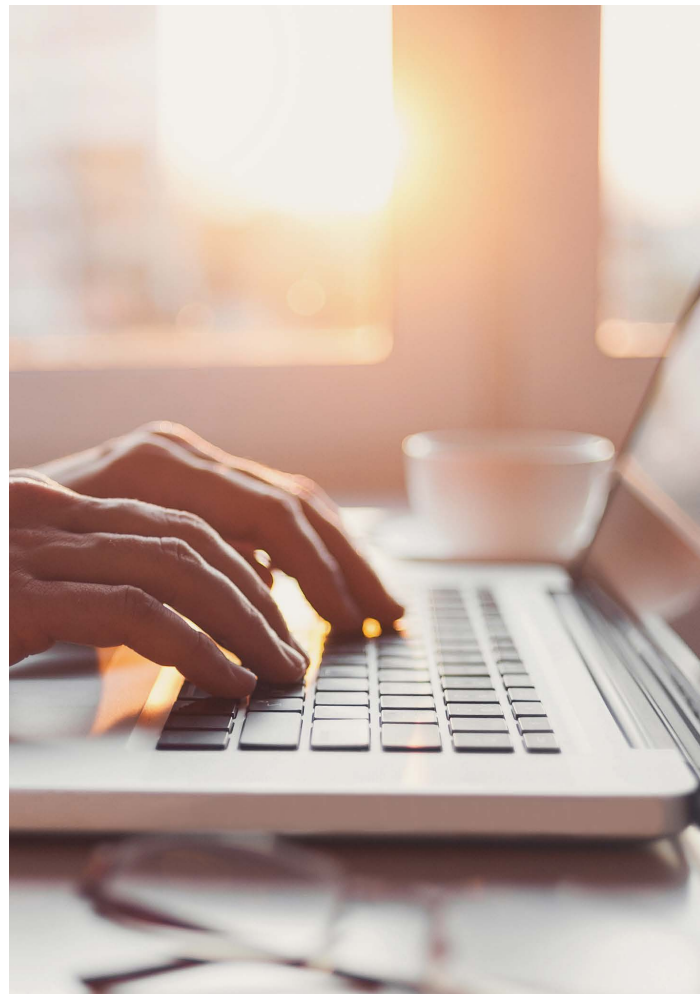
## CYFOR

We are instructed by clients from a full spectrum of industries and offer a bespoke solution on highly contentious, multi-lingual and multi-jurisdictional matters with time critical deadlines.

Our ability to combine specialist digital forensic techniques with each stage of the eDiscovery life-cycle gives us a proven capability from extraction through to production.

Individually, CYFOR's expert analysts are recognised as some of the leading specialists in the industry. As a team, their combined expertise becomes even more powerful for the most complex of cases. This breadth of experience is combined with a highly secure ISO 27001 certified infrastructure.

For more about CYFOR visit:  
[www.cyfor.co.uk](http://www.cyfor.co.uk)



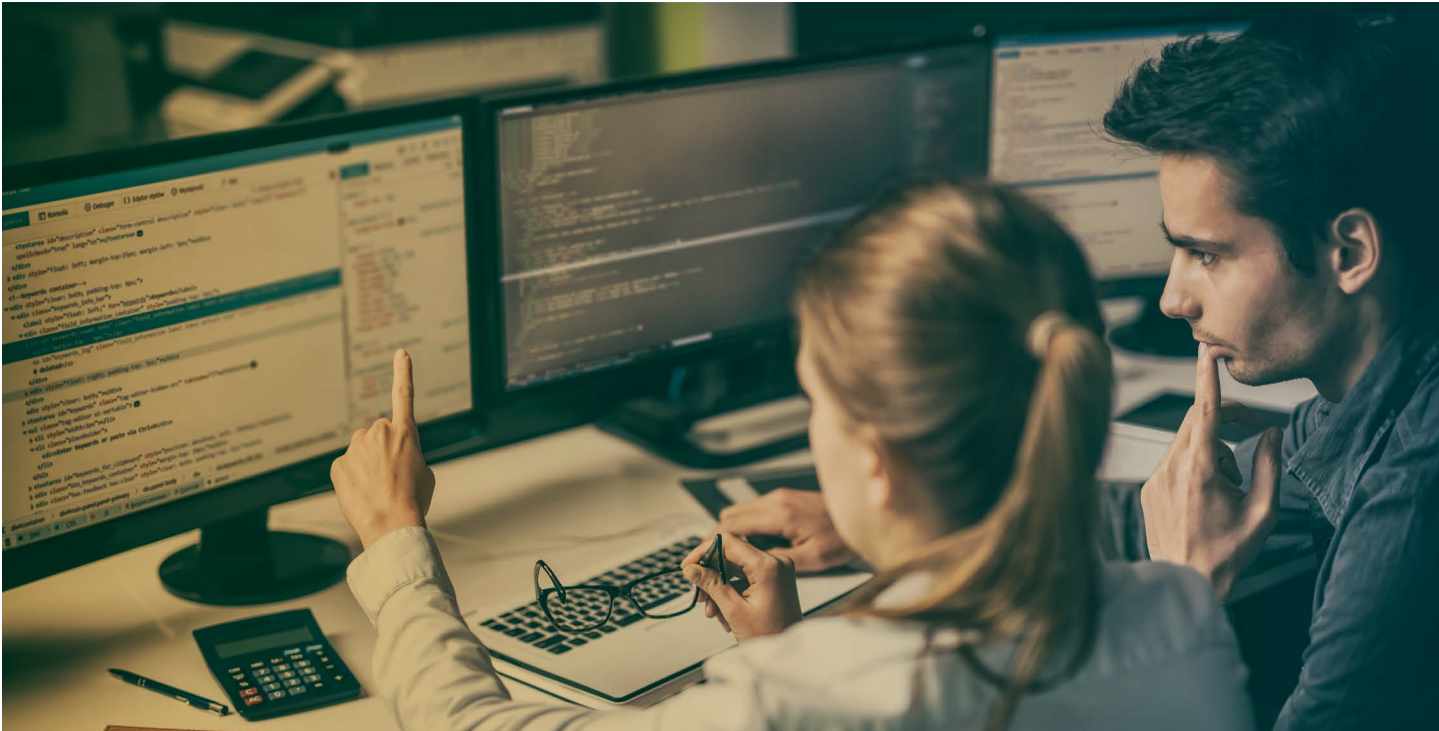
# Appendices

## 1.1

As a starting point the researchers focused on the most valuable 50 UK brands, as identified at the end of 2017<sup>18</sup>. These were as follows:

- |                 |                                    |                                 |
|-----------------|------------------------------------|---------------------------------|
| 1. Shell        | 18. Sainsbury's                    | 35. BAE Systems                 |
| 2. Vodafone     | 19. Dove                           | 36. SSE                         |
| 3. HSBC         | 20. Standard Chartered             | 37. NatWest                     |
| 4. BP           | 21. Johnnie Walker                 | 38. Royal Bank of Scotland      |
| 5. EY           | 22. Aviva                          | 39. GlaxoSmithKline             |
| 6. Barclays     | 23. EE                             | 40. Holiday Inn                 |
| 7. BT           | 24. Unilever                       | 41. Aon                         |
| 8. Tesco        | 25. Marks & Spencer                | 42. Morrisons                   |
| 9. Sky          | 26. Burberry                       | 43. Walgreens<br>Boots Alliance |
| 10. O2          | 27. Virgin media                   | 44. MINI                        |
| 11. Booking.com | 28. BHP                            | 45. Royal Mail                  |
| 12. ASDA        | 29. Prudential (UK)                | 46. British Gas                 |
| 13. Land Rover  | 30. British Airways                | 47. Scottish Widows             |
| 14. Pall Mall   | 31. Rolls-Royce                    | 48. Lipton                      |
| 15. Lloyds      | 32. Nationwide<br>Building Society | 49. Compass Group               |
| 16. 3 Mobile    | 33. ITV                            | 50. Rio Tinto                   |
| 17. BBC         | 34. Halifax                        |                                 |

<sup>18</sup> [http://brandirectory.com/league\\_tables/table/uk-150-2017](http://brandirectory.com/league_tables/table/uk-150-2017)



## 1.2

The researchers searched Dark Web areas known as 'Market Places', identifying those which were sufficiently stable to search while also being popular enough for what was found to be representative.

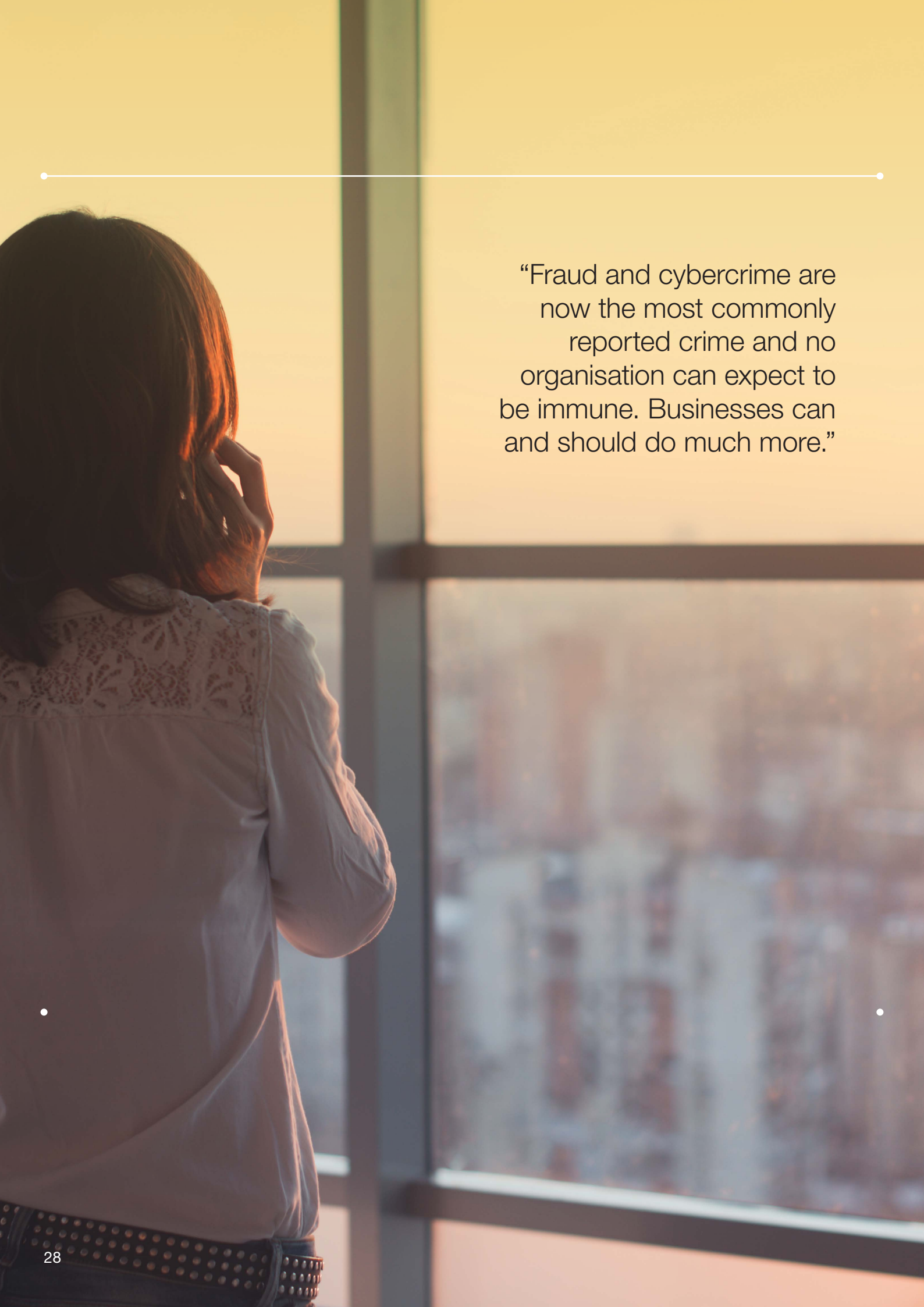
## 1.3

Searches were undertaken across the following 'Market Places'.

- Dream Market.
- Wall Street Market.
- Olympus Market.
- Point/Tochka.
- Rapture Market.

## 1.4

Researchers then looked beyond the top 50 UK brands and found a large number of other brands being discussed.



“Fraud and cybercrime are now the most commonly reported crime and no organisation can expect to be immune. Businesses can and should do much more.”





## Start the conversation

Jim Gee  
Partner  
National Head of  
Forensic Services

[jim.gee@crowe.co.uk](mailto:jim.gee@crowe.co.uk)  
+44 (0)20 7842 7239

## About Us

Crowe UK is a national audit, tax, advisory and risk firm with global reach and local expertise. We are an independent member of Crowe Global, the eighth largest accounting network in the world. With exceptional knowledge of the business environment, our professionals share one commitment, to deliver excellence.

We are trusted by thousands of clients for our specialist advice, our ability to make smart decisions and our readiness to provide lasting value. Our broad technical expertise and deep market knowledge means we are well placed to offer insight and pragmatic advice to all the organisations and individuals with whom we work. Close working relationships are at the heart of our effective service delivery.

[www.crowe.co.uk](http://www.crowe.co.uk)

  @CroweUK

Crowe U.K. LLP is a member of Crowe Global, a Swiss Verein. Each member firm of Crowe Global is a separate and independent legal entity. Crowe U.K. LLP and its affiliates are not responsible or liable for any acts or omissions of Crowe Global or any other member of Crowe Global.

© 2018 Crowe U.K. LLP | 0071