REPRINT

R&C risk & compliance

CYBER FRAUD TYPOLOGIES AND ACTIONABLE INTELLIGENCE

REPRINTED FROM:
RISK & COMPLIANCE MAGAZINE
JUL-SEP 2019 ISSUE

www.riskandcompliancemagazine.com

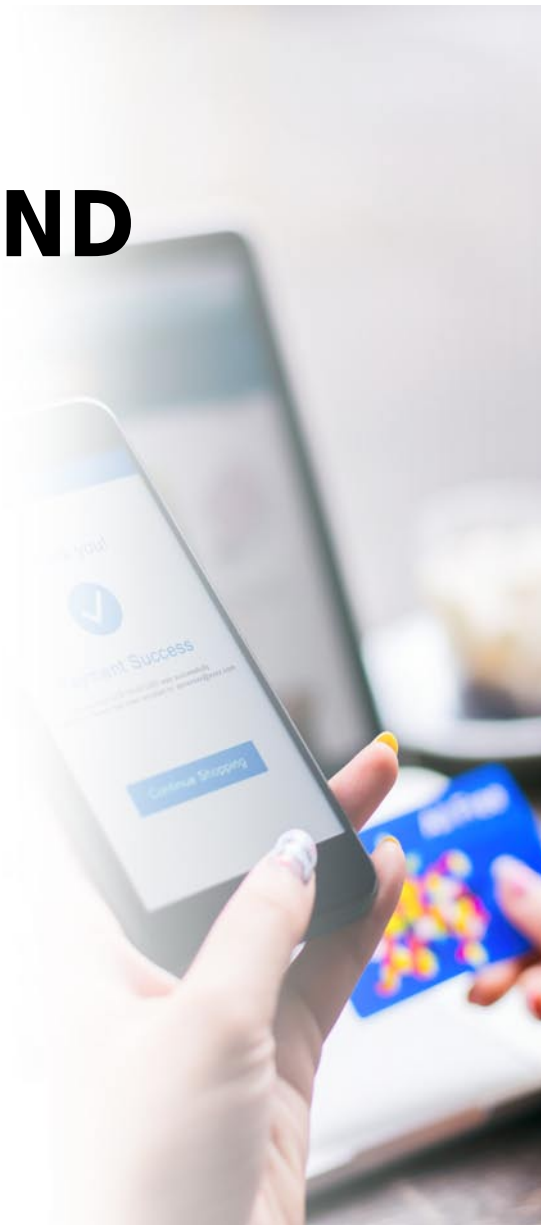
Visit the website to request
a free copy of the full e-magazine

Acuris Risk Intelligence

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com

ONE-ON-ONE INTERVIEW

CYBER FRAUD TYPOLOGIES AND ACTIONABLE INTELLIGENCE



Nick Parfitt
Head of Market Planning
Acuris Risk Intelligence
T: +44 (0)20 3741 1200
E: info@acuris.com

Nick Parfitt is responsible for determining Acuris Risk Intelligence's approach to the market and building subject-matter expertise. He has 18 years' experience in project and programme management, business process change and in implementing technology and business solutions at financial services, telecoms and public sector organisations. His experience in the financial crime sector spans seven years helping tier 1 financial institutions assess and improve AML, KYC and sanctions operations. Mr Parfitt has worked for several tier 1 banks in the UK and holds an MBA (Distinction) from Cardiff University, and a BA (Hons) in Biochemistry from Imperial College.

R&C: Could you provide an insight into the current fraud trends facing consumers? How have the risk dynamics evolved in recent years?

Parfitt: Levels of fraud and cyber attacks continue to increase year-on-year, although the typologies and levels of activity tend to wax and wane as businesses, regulators and the industry at large play a cat-and-mouse game with criminals and organised crime. According to UK Finance, in 2018 "the advanced security systems and innovations in which the finance industry invests to protect customers stopped more than £1.6bn of unauthorised fraud. But despite this, criminals successfully stole £1.2bn through fraud and scams." In the UK, we have seen a big increase in 'Authorised Push Payment' (APP) scams, which were up 93 percent for 2018 compared to 2017. Card not Present (CNP) and remote purchase and Card ID Theft accounted for the biggest increases since 2017: 47 percent and 119 percent respectively. Interestingly, we are seeing a lot of PPI-related information in our data, which suggests that criminals are either targeting PPI firms, or PPI firms that are no longer active have been selling their customers' data either knowingly or unknowingly to criminals.

R&C: What methods are criminal organisations using to target consumers and businesses to commit cyber fraud?

Parfitt: Beyond general hacking activities to obtain email addresses, passwords, card details and so on, we see criminals advertising goods and services on social media in order to steal card details and personal information. Criminals also use websites that purport to offer genuine services, such as advice on debt management, to lure the unsuspecting public to provide sensitive personal details such as name, date of birth, mother's maiden name, address information and the financial institutions with which they have relationships. For businesses, invoice and 'CXO' frauds are highly prevalent and growing, with a 2018 UK Finance report showing that in the first six months of 2018 there were 2856 cases of invoice and mandate fraud. Invoice fraud involves convincing the business to change account payee details for payment, with the criminal posing as a regular supplier. CXO fraud generally involves criminals gaining access to a company's email system or 'spoofing' an email address to make it look as if the message has come from a particular executive.

R&C: What are the typical business vulnerabilities that cyber criminals are exploiting for fraudulent purposes? In your experience, how aware are companies and their employees of such vulnerabilities?

Parfitt: Business vulnerabilities include criminals using the unindexed web to search for 'cracked passwords', trading email addresses and exploiting home and public Wi-Fi routers – and the low-tech option of impersonating employees to gain physical access. In a recent example of 'social engineering', an attacker posing as someone delivering food to an office was able to slip a USB device into a local printer. Within minutes, the attacker had full access to the corporate network. Luckily, this was just a test to show vulnerability. Awareness varies enormously and can also be time-limited. Immediately after security training, people are aware and alert, but fast-forward three to six months and they tend to forget about the risks and return to default 'trusting' behaviours. However, with the implementation of the European Union's (EU's) General Data Protection Regulation (GDPR), there is a generally good understanding of the importance of client data and the need for it to remain as secure as possible.

R&C: Could you highlight any recent fraud-related cyber incidents which illustrate the magnitude of these risks?

Parfitt: In November 2018, a major airline suffered a data breach that impacted customer information from approximately 380,000 booking transactions. It exposed data such as card verification values (CVVs), even though the airline does not store this information. In March 2019, one of the world's largest aluminium producers was hit by a ransomware attack, forcing it to partially cease operations. These incidents highlight the damage that hackers can cause to critical infrastructure and industrial systems, as did the 2017 'WannaCry' ransomware attack, which caused significant damage to hospitals, banks and companies worldwide. Most recently, a marketing company that offered 'enterprise email validation' services was hacked, leaking 982 million email addresses. The breach included other personal information such as employer, date of birth, names, gender and social media accounts and physical addresses.

R&C: What can consumers and businesses do to protect themselves? What do you consider to be the essential components of an effective cyber security strategy to fight fraud?

Parfitt: For consumers, we would recommend people first be aware of fraud typologies and threats, and then limit their digital exposure as much as possible and question the information that they are being asked for. Does a gaming website really need my date of birth? There are a few companies offering to check and monitor consumers' exposure to the 'dark web' which can be bundled with a credit reporting and checking facility. This shows what your current and potential cyber threat may be. Beyond that, ensure passwords are unique,

strong and changed regularly, always use a virtual private network (VPN) and 'harden' home networks. Businesses should also be looking to understand whether they have any exposure on the dark web, by looking at email domain addresses to see whether criminals are, or have been, targeting them. The same goes for company usernames and passwords. Phishing attacks are increasing and businesses can screen all incoming emails against known 'temporary' email domains to red-flag potential attacks, but education is one of the best defences. Having IT departments send emails that mimic phishing attacks and then tracking internal responses is a good way of showing the importance of vigilance.

R&C: What general tips would you offer in terms of tailoring cyber risk management to the specific needs of an individual or business? How can technology help?

Parfitt: As an individual, assess what you do online and how a hack or online identity fraud might impact you, particularly if you use internet banking and access many different e-commerce sites where your credit or debit cards are regularly used for payments. If you are highly active, look to protect yourself as much as possible. Businesses need to balance their size and attractiveness as a target with their strategies to counter cyber attacks. But any company that is hacked is subjected to potential fines, reputational risk exposure and painful remediation actions. Artificial intelligence (AI) and behavioural-based anti-malware software offers superior benefits when compared to traditional anti-virus software, as it can assess and monitor abnormal file and operating system changes.

> **"Artificial intelligence (AI) and behavioural-based anti-malware software offers superior benefits when compared to traditional anti-virus software."**
>
> *Nick Parfitt, Acuris Risk Intelligence*

R&C: Looking ahead, do you expect consumers and businesses to devote more time and attention to protecting themselves from cyber-related fraud? What innovations are on the horizon to help them do so?

Parfitt: With ever-increasing and high-profile cyber attacks being reported in the press, hopefully consumers are taking their data security ever more seriously. It is good to see public initiatives such as 'Take Five to Stop Fraud' raising public awareness, but much more needs to be done. Also, we are beginning to see banks offering better protection and awareness, as well as signing up to new initiatives such as the 'authorised push payment scams' voluntary code. With many businesses there are varying degrees of maturity, most likely driven by lack of awareness. However this needs to change, particularly given the GDPR implications. With a recent report by the Department for Digital, Culture, Media and Sport stating that 32 percent of businesses and 22 percent of charities identified cyber security breaches or attacks in the last 12 months, the problem for UK businesses is significant and should not be underestimated. AI and behavioural-based anti-malware solutions are offering new levels of capability, but as the Internet of Things (IoT) gains more traction, it will become more difficult to manage cyber threats, particularly for consumers. Technology can help. But it is what each of us can do, both for ourselves and the organisations we work for, that is likely to make the most impact, especially if we know what our cyber exposure is at any given time. R&C