FINANCIAL CRIME SOLUTIONS

Business fraud report: global

2018–2019

Contents

Introduction

David Rich
Executive Vice President
Real-time Services

Welcome to our third annual business fraud report, which explores awareness levels and attitudes to payments fraud in the UK, US and – for the first time – Australia.

In recent years, payments fraud such as invoice redirection, mandate fraud, and CEO/business email compromise fraud have become an increasingly popular way for fraudsters to extort money. Businesses large and small can fall victim to these types of scam – and our report shows that bosses are often shocked by the extent of criminal activity and scale of losses, believing that fraudsters are now one step ahead.

Companies reporting that payments fraud has been attempted on their business, or who have fallen victim to it, are all too common and official figures suggest this type of scam is on the rise. Fraud can have a devastating impact on a business, leading to owners questioning whether they should continue to own their business, contemplating closure, and even leading to the breakdown of relationships with friends and family.

It's vital that we do all we can to combat these types of fraud. This is a global issue, however, which requires industry-level collaboration if we're going to make a positive change. Tackling fraudsters and money launderers is now a number one priority for many financial institutions, crime prevention agencies and governments around the world.

We have developed a suite of services using technology – which overlays card and account payments data with leading data science tools and techniques – to develop analytic and consulting solutions that protect legitimate users of payments systems.

Our solution to prevent business payment fraud analyses tens of millions of transactions to identify high risk payments which display business payment fraud characteristics. We are also helping to combat mule accounts and money-laundering with our solution to trace financial crime across payment networks. This is now live in the UK, tackling and tracing stolen and illicit funds as they are dispersed across the system. Our technology can be applied to payment systems around the world, or within specific organisations, delivered via our micro-service-enabled cloud platform, which enables the swift deployment of our services and solutions.

We have developed these solutions because we believe in thoughtful innovation that can power economies and empower people. This doesn't just mean innovating to be disruptive – we strive to constantly improve and evolve our solutions also. They are designed to continually adapt to the changing environment, and as fraudsters find increasingly sophisticated ways to exploit others. This should provide reassurance that we are working with our customers to continue to invest in the development and deployment of financial crime solutions that tackle some of the biggest issues impacting people, businesses and economies.

In the meantime, our research shines a light on the current experience of business owners and should encourage the authorities, the financial sector, and businesses across the globe to continue working together in the fight against payments fraud.

What is the ‘Business fraud report’?

Our annual Business fraud report is considered the definitive account of payments-related fraud in both the US and the UK. This year, for the first time, we included Australian businesses in our research.

The report canvasses entrepreneurs, business owners, managers and directors on their response to, and experience of, the following types of payments fraud:

CEO fraud

Where cybercriminals use social engineering to impersonate executives and trick other employees into executing unauthorized wire transfers or sending tax and sensitive information.

Business email compromise fraud

A sophisticated scam in which fraudsters gain access to, or spoof, internal email addresses (sometimes called ‘man-in-the-middle’ email). They often target businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments.

Invoice redirection and mandate fraud

High-value fraud targeting companies where false payment invoices and payment directions are sent to a supplier’s customer.

The issue of payments fraud for companies

Payments fraud occurs when companies pay money erroneously to a fraudster rather than a legitimate supplier. Once processed, the funds are laundered rapidly through the banking system making them difficult to trace. Stolen funds are rarely recovered, leaving financial institutions, and sometimes their customers, to bear the cost.

Payments fraud includes invoice redirection, mandate, CEO or business email compromise (BEC) fraud and email account compromise (EAC) fraud. For example, a supplier's email account may be spoofed and used to request payments from the company into a new bank account, or a fraudster may pose as the CEO and send an email to employees in finance, requesting them to transfer money to a particular account. Scammers are extremely adept at finding ways to get people to act, such as communicating an extreme sense of urgency which pressurises victims into carrying out the requests quickly and without making any routine checks.

Businesses have become an increasingly popular target for fraudsters as they realise that there are large gains to be made. Globally, the BEC/EAC scam continues to grow and evolve, targeting small, medium, and large business and personal transactions. The following BEC/EAC statistics were reported to the FBI's Internet Crime Complaint Centre (IC3) and are derived from multiple sources, including IC3 and international law enforcement complaint data and filings from financial institutions between October 2013 and July 2019:

- Domestic (US) and international incidents: 166 thousand
- Domestic (US) and international exposed dollar loss: $26 billion

However, this is likely to represent only a part of the picture, as often payments fraud is underreported with some victims simply too embarrassed to come forward.

This is our third annual report that investigates levels of awareness and attitudes to different types of payments fraud. This year's research was expanded to feature Australian businesses for the first time, building on previous the years' UK and US reports. Businesses of all sizes were surveyed; small, medium and large, to assess how different types of payments fraud such as invoice, mandate and CEO fraud have impacted everyone from entrepreneurs to the largest organisations.

Key research findings

Fraudsters are winning

66% of business bosses in the US, Australia and the UK are shocked by the extent of losses suffered by the business community. 70% believe that the fraudsters committing invoice redirection, mandate and CEO fraud are now 'ahead of the industry'.

Impact on owners' health

Business owners in both large and smaller businesses who have fallen victim to modern-day payments fraud, or knew a business that has, said that their health and wellbeing was compromised due to high levels of stress, frustration and feelings of helplessness:

- 46% said it has impacted their stress levels.
- 31% felt helpless because they didn't know where to turn for help.
- A quarter (25%) said it negatively affected their health and wellbeing.
- 10% even said they had considered suicide as a result.

A cry for help

While banks and industry bodies have already run campaigns to raise awareness of this issue, business owners are calling for more practical help to fight fraud. Many admit they don't know enough about how fraudsters are able to carry out these attacks and would like greater support:

- 43% of business owners are concerned they don't possess enough personal knowledge to protect their business from payment-related fraud.
- 79% of businesses want the banks and government to do more to protect businesses.

The results in detail

The most surprising and concerning findings show that, while a large number of businesses across the three countries believe payment-related fraud is becoming a bigger issue, they haven't made any changes as a result. Lack of time and money to train staff was cited as one reason.

1. 38% of business owners have either been a target of attempted payment-related fraud, or know a business which has, and lost thousands of dollars/pounds in the process. 11% of owners contemplated closing their business as a result.
2. While awareness of the crippling impact of payment-related fraud has improved among businesses, 33% still admit that they are unaware of mandate, invoice redirection and CEO fraud. That's almost 11.8m businesses across Australia, the UK and the US (this is based on a total of 27.6m businesses in US, 2.6m in Australia and 5.7m businesses in UK).
3. 56% of business owners agreed that payment-related fraud became a bigger issue for them in 2018. Despite this, however, 35% of businesses admit they haven't tightened accounting processes and 20% made no changes to their overall business in 2018 to identify and tackle fraud.
4. 81% of business owners were surprised that there is not more news or information available about the extent of losses due to payment-related fraud, with 72% believing that payment-related fraud isn't getting enough media attention.
5. 29% admit that their employees are not trained to identify fraudsters and 24% don't have the time or money to spend on training.
6. 30% wouldn't know who to turn to if it happened to them with 44% stating that they don't believe the police take this type of fraud seriously.
7. 17% of bosses and entrepreneurs who have had to deal with the fall-out from crippling payments fraud cited problems with their relationships with family and friends as a result.
8. 37% believe the banks hold the most responsibility when it comes to combating payment-related fraud.

How do we solve this problem?

Our financial crime solutions overlay large-scale payments data with cutting-edge data science tools and techniques which are trained on over 20 billion transactions amounting to trillions of pounds in value, to protect the legitimate users of payments systems.

We prevent business payment fraud using advanced, self-learning and behavioural analytics. On a daily basis, our solution analyses tens of millions of transactions to identify high risk payments which fit the characteristic of these types of frauds early in the transactional cycle and deliver a manageable number of alerts, precisely tuned to a customer's preference. It is already live in the UK, and as at September 2019 it had prevented NatWest business customers from losing £14.5 million to fraudsters.

We can also trace financial crime at a network-level, within and between bank and building society accounts regardless of whether the payment amount is split between multiple accounts, or if those accounts belong to the same or different financial institutions. Our solution provides additional intelligence beyond an individual financial institution's partial view. Already live in the UK through a partnership with Pay.UK, this is a significant step-up in fraud decision and anti-money laundering analytics.

Given that financial services fraud is such a major, global issue, it's clear that we need a multi-channel approach to tackle it. It requires combined action from governments, banks, regulators, businesses and payment-systems providers to combat this problem.

There is a huge amount of work already happening in this space but clearly more that needs to be done, particularly around raising awareness. In the meantime, there are some steps that businesses can take to protect themselves:

1. **Be vigilant** – Make business fraud the business of everyone, not just the accounting teams. Train client-handling or account-facing teams about the risks and implications of business fraud, and how to identify the signs.
2. **Authenticate** – Verify any requests from the MD, CEO or board through a tiered system where emails and telephone conversations requesting movement of monies are verified by a second trusted contact.
3. **Introduce checks** – Instigate checking of communications amongst finance and account-handling teams such as email addresses, use of English, and written mistakes in the email. Encourage a system whereby suspect emails are checked by a second team member.
4. **Protect** – Anti-virus software should be kept up to date, and computer systems must be secure. This is not an additional cost but an essential part of day-to-day business practice.
5. **Be alert** – Pay special attention to any request from suppliers or clients for payment details to be changed, especially via email. Fraudsters will often use social engineering to trick staff into updating details. Employ a secondary validation process by calling a known number/contact at the supplier to verify the request is legitimate.

i www.ic3.gov/media/2018/180712.aspx
ii www.census.gov/search-results.html?q=number+of+businesses+in+us&page=1&stateGeo=none&searchtype=web&cssp=SERP&_charset_=UTF-8
iii www.abs.gov.au/ausstats/abs@.nsf/mediareleasesbyReleaseDate/B511DD61F9656CF9CA25823900112DDB?OpenDocument
iv researchbriefings.files.parliament.uk/documents/SN06152/SN06152.pdf

Financial crime solutions

Our award-winning financial crime solutions help our customers better verify payment requests and recipients and prevent financial crime before it occurs. Our network-level solutions allow us to trace illicit funds across the payments network and alert financial institutions to suspect mule accounts so they can investigate and close them down. They can be engaged either at individual bank or scheme level, or across entire payment networks anywhere in the world.

For more information

vocalink.com/financialcrimesolutions
info@vocalink.com

"This is a global issue that requires industry collaboration"

Contact us
info@vocalink.com
vocalink.com

Head Office
1 Angel Lane
London
EC4R 3AB
United Kingdom

740057/03.111019

DESIGNED BY NPP CREATIVE