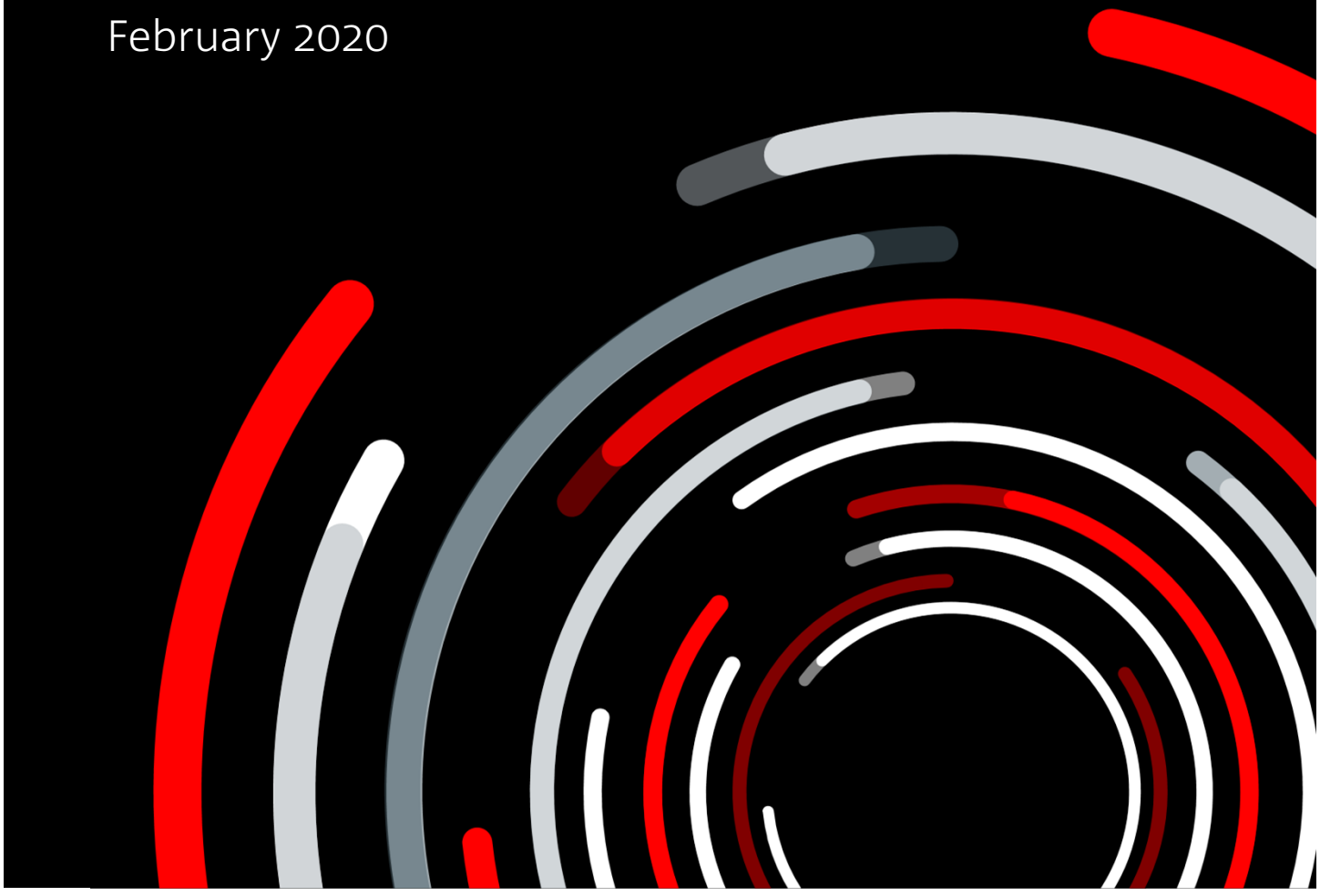
more than money

nab

PAYABLES FRAUD

A growing problem in Australia

February 2020



more than money

nab

Payables Fraud
A GROWING PROBLEM IN AUSTRALIA

Fraud threats to organisations are becoming increasingly sophisticated and targeted. Technology is enabling criminals like never before, with examples of artificial intelligence and voice technology now being used to accurately impersonate business owners, defrauding organisations globally of millions. At NAB, we see fraud incidents regularly across our corporate and institutional customers and losses can range from small to large reportable events. All however, can typically relate back to failures of system, people or process.

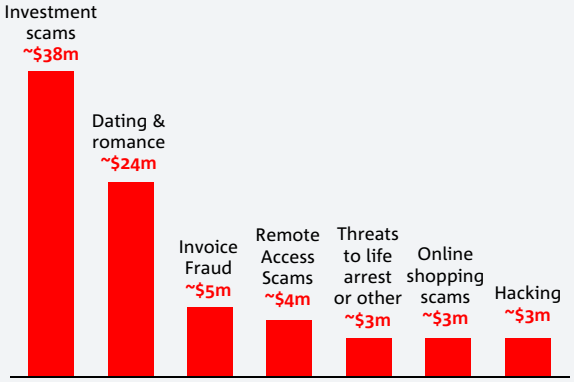
The statistics do not capture a large proportion of unreported events, however for some context, a snapshot of top scams from a recent ACCC report puts invoice fraud for businesses in the top 3 by value (see graph below).

When combined with data from other agencies, the reported losses to business email scams alone in Australia exceeded $60 million in 2018. This is a **170% increase over the losses reported in 2017.** (ACCC Targeting Scams report 2018)

Some types of threats that Australian corporates face include:

- **Phishing ('fishing'):** usually happens in the form of an email, often appearing to be from a senior executive, requesting for an urgent funds transfer.
- **Business Email Compromise (BEC):** a business may receive an email invoice from a supplier asking for payment. If the supplier's email account has been compromised, the email may be intercepted and the payment details on the invoice changed.
- **Ransomware:** software that once executed, encrypts (locks) all the files on a computer. The victim then receives a demand for a ransom to be paid to access their files.
- **Data breaches:** information held on databases or payment gateways that is not well protected may be accessed by hackers. This information is usually on-sold via hacker websites or on the black market.
- **Advanced persistent threats:** where an intruder gains access to an organisations IT environment and remains for a prolonged period monitoring activity and accessing sensitive data.
- **Social engineering:** the targeting of employees in their personal lives to capture login details or personal information that can help a criminal gain access to an organisations environment.

Top scams by loss, 2018



Source: 'Targeting scams: report of the ACCC on scam activity 2018'.

PAYABLES FRAUD
A GROWING PROBLEM IN AUSTRALIA

Having up-to-date technology systems and good resilience against cyber-based threats is important for organisations today.

However, given Phishing and BEC are key areas of weakness within finance teams for payables fraud in Australia, we will explore these concepts and highlight some measures to mitigate the risk.

Please note, we also do not cover internal fraud risk within this paper – another important layer of governance and control consideration for corporates.

Phishing

Our historical perception of email scams is typically of a poorly worded request, usually very easy to spot. Today, finance staff can find it increasingly difficult to pick the differences from a legitimate email. If the senders' systems have been compromised, it could actually look quite legitimate.

Usually the fraudster will be impersonating a senior manager and will be asking for (usually) a funds transfer to an account. Reasons can vary but almost always have a sense of urgency about them. The target will be someone in a role that can action payment creation within the organisation and has some distance from the senior levels (by structure or geography).

There are several things that could still standout to the vigilant employee however:

- Not from a known email address;
- No greeting – not personalised or a generic greeting;
- Unfamiliar phrases and poor language;
- Designed to panic/annoy – sense of urgency;
- No contact details provided;
- Embedded links; and
- Old/incorrect branding.

Case Study #1

- A large corporate was defrauded through a coordinated scam. Firstly, the account details on an invoice were changed and emailed from a similar looking supplier email address, copying the invoice layout effectively. These details were then updated on the vendor record for that supplier by a staff member without further scrutiny.
- The account details provided in fact belonged to the victim of a romance scam. They had been manipulated at length by the fraudsters, posing as an individual interested in a personal relationship with the victim. The victim, believing that funds arriving into their account were legitimate, had instructions on where the value was to be transferred (offshore).
- The corporate was eventually advised by the supplier that value was missing, which triggered an investigation. By this time, funds had left Australia from the victims account, whose owner was also impacted, both financially and personally.

"Having up-to-date technology systems and good resilience against cyber-based threats is important for organisations today."

PAYABLES FRAUD
A GROWING PROBLEM IN AUSTRALIA

Business Email Compromise (BEC)

BEC is a significant issue, largely due to legacy processes that typically exist, within large organisations. Across supplier onboarding and validation, governance and change controls and staff awareness of the red flags for fraud, many Australian organisations in this country are vulnerable to attack from internationally based criminals. These parties are organised, technically capable, well resourced and singularly focused on their objective.

Ensuring good governance and controls are in place within a corporate finance team is critical to combat this threat. At a basic level, NAB recommends the following steps are explored in the first instance.

1. Make sure your systems are secure, with up to date virus protection.
2. Protect your business data by regularly backing up, storing offsite and testing the backups regularly.
3. Be vigilant on passwords and access management for all staff.
4. Ensuring appropriate transaction controls within electronic banking such as segregation of duties and/or dual authorisation.
5. Be on the lookout for suspicious emails as part of the normal course of business.

Fundamentally for payables teams, we recommend that any requested change to supplier details, particularly a change to bank account information are validated directly with a known contact at the supplier. Additionally, for suppliers that are legitimately seeking to update bank account details with their customers, proactive messaging via several channels ahead of any change being formally communicated is recommended to avoid confusion and to ensure a seamless migration.

Case Study #2

- Low governance controls meant one email password was shared amongst the Accounts Receivable team at a supplier. These details fell into the hands of a Fraudster.
- The Fraudster monitored emails and intercepted a real invoice emailed to a customer and manipulated the bank account details within. A follow-up email was quickly sent to the same customer by the fraudster from within the suppliers hacked email, advising that the original invoice contained an error and attached a changed invoice.
- As this was from a known email address for that supplier, the customer did not validate further and makes a payment to the account number specified in the altered invoice.
- The bank account used for the fraud was a legitimate account of a retiree. They had been manipulated into disclosing their personal internet banking details by the fraudsters, ultimately providing full online access to the account.
- The supplier queried the missing funds two weeks later, triggering a review and investigation. This represented a total loss for the suppliers' customer as funds had already moved offshore.

Payment solutions to mitigate fraud

Increasingly, businesses have other options to include within an automated suite of payables options to add more control and certainty of funds reaching their intended beneficiary. Whilst even an attempt to update account details incorrectly is already a failure of process, some payment channels will present a better 'final test'.

A traditional overnight payment contains very few controls for payers. A BSB and account number can very easily be modified at various stages and there are few options available to validate the destination of the funds. Once a payment has been processed, it is then a long process to retrieve value and is likely to have already disappeared. Other options for business to consider are below.

- **BPAY:** an established option in the payments landscape in Australia is BPAY. Many businesses accept BPAY today for the reconciliation automation benefits. For business payers, if using a BPAY batch payments file, multiple BPAY payments can be created and released as part of a standardised batch payables process. The use of a bank sponsored BPAY Biller code by the beneficiary, provides certainty of the ultimate destination being with a legitimate business and is therefore unlikely to be a scam linked bank account, mitigating the likelihood of fraud.
- **Fast Payments:** the New Payments Platform (NPP) launched in 2018 enables what NAB calls Fast Payments. This is real-time value, transferred 24/7 domestically. Whilst that seems a high-risk proposition, the difference is the addressable details that are available to the payer before the transaction occurs. Via the NPP, a payer can input the account (or PayID) details and retrieve immediately the name of the legal owner of the destination account from the account holder's bank. This provides an opportunity to perform final hygiene on a payment before it is released.
- **Corporate Cards:** cards are widely acknowledged as a more convenient and cost-effective tool for payables. Traditionally organisations have not scaled their use beyond travel and general purchasing, largely due to a card transaction being typically manual, with controls being after the spend has occurred. Through the introduction of pre-spend controls to corporate cards at NAB, these can now be made available to a broad range of users. Associating more spend to authorised cardholders, reduces what might have been processed via legacy procurement and payables channels, providing secure cost savings for the business.
- **Automated Invoice Payments:** NAB can support the bulk processing of invoices to validated suppliers via a card facility, aligning to a traditional batch payables process. This ensures certainty of value reaching the beneficiary, as a live merchant facility gives comfort that the suppliers bank has validated the business and the purpose of the facility. Underpinning that, are additional chargeback rights and protections afforded by the card scheme network. Changes to details for onboarded suppliers cannot be modified without appropriate approval. Organisations have effectively outsourced the bank account details aspect of vendor management to the bank, and can explore mutually beneficial working capital arrangements with suppliers within the solution.

"Businesses have other options to include within an automated suite of payables options to add more control and certainty of funds reaching their intended beneficiary."

PAYABLES FRAUD
A GROWING PROBLEM IN AUSTRALIA

Conclusion

Good fraud prevention measures can help avoid not only direct costs such as loss of value and remediation activities, but also indirect costs such as downtime, lost productivity and loss of reputation.

A mixture of fraud prevention measures across an organisation, controls for technology, clear processes for finance teams and a good level of risk understanding in today's market is important for all businesses to prioritise.

Not every mitigation strategy will be suitable but strategies need to form part of a holistic approach to fraud mitigation. Organisations should consider their unique business requirements and risk environment when deciding which mitigation strategies to implement. Furthermore, before any strategy is implemented, comprehensive testing should be undertaken to minimise any unintended disruptions to the organisation's business.

A good reference for further technical fraudulent email mitigation strategies can be found on the Australian Signals Directorate website. You can also report if you have been a victim of a scam or cybercrime: https://www.cyber.gov.au

And to stay up to date on current scams: http://www.scamwatch.gov.au

Author

Shawn Treloar
NAB Director Customer Solutions & Strategy

Shawn has worked in transactional banking for over 10 years, and is currently working within the Customer Solutions team, identifying opportunities for business development across NAB's Corporate & Institutional Banking sectors.

Shawn has a technology background and a passion for enhancing business operations with tech solutions. Shawn is a graduate from the Queensland University of Technology and holds a Bachelor of Business in Management and Electronic Business.