



# Safeguarding Your Property Settlement: Awareness and Prevention of Scams

**White Paper, Scam Awareness Week 2025**

By Graham Fairley

Chief Information Security Officer, PEXA

# Contents

<b>Introduction</b>	1
<b>The Rise of Property Settlement Scams</b>	2
How Property Settlement Scams Work	3
<b>Staying Safe: How to Protect Yourself</b>	6
Roles and Responsibilities: Who Needs to Manage the Risk?	7
Home Buyers and Sellers	7
Conveyancers and Solicitors	8
Financial Institutions (Banks and Lenders)	8
PEXA and Digital Platforms	9
<b>Conclusion</b>	12
Additional Information	13

# About PEXA

PEXA is an Australian innovation, the world's first and leading digital property settlement and lodgement platform.

Borne out of a public-private partnership over 15 years ago, today it is an ASX-listed company that employs more than 1000 people in Australia and the UK and has transformed the Australian property market. Property settlements that were once antiquated, paper-based and time-consuming processes are today a seamless, digitised and secure solution that provides significant time and cost savings to Australian property buyers and sellers.

PEXA works with around 11,000 Australian conveyancers and legal practitioner firms and connects more than 160 financial, government and statutory bodies on its network.

# About the Author



**Graham Fairley**

Chief Information and Security Officer, PEXA Group

Graham has held the role of PEXA CISO since 2024. He has been a leader in cyber security for more than 20 years with proven expertise in developing and executing comprehensive cybersecurity and technology risk management strategies aligned with business objectives. He is adept at safeguarding organisational assets through effective governance frameworks, incident response, and cross-functional collaboration. As PEXA's CISO, Graham is responsible for leading the security program to prevent intrusions and protect its customer data.

# Introduction

Scam Awareness Week 2025 calls on Australians to “*Stop. Check. Protect.*” to keep ourselves safe from fraud<sup>1</sup>. During this national awareness week, PEXA’s Chief Information Security Officer (CISO), Graham Fairley, shines a light on a growing threat in the property industry, **property settlement scams**, and how the community can combat them.

Buying or selling a home is one of the biggest financial transactions most people will ever undertake, and cybercriminals have taken notice.

This white paper outlines the common tactics scammers use in property settlements, shares insights from recent market research on public awareness, and provides practical steps for buyers, sellers and professionals to mitigate the risks.

# The Rise of Property Settlement Scams

Property settlement scams have become one of the most financially devastating forms of cybercrime in Australia. These scams, typically executed via business email compromise (BEC), involve criminals impersonating real estate agents, lawyers, or conveyancers to trick buyers or sellers into transferring funds to fraudulent accounts during a property settlement.

But there are ways to protect yourself.

The scale of these attacks is growing rapidly. In one Western Australian case, a homebuyer lost **\$732,000** after cybercriminals hijacked email communications and inserted false bank details. In Sydney, a couple unknowingly transferred **\$970,000** to scammers during what they believed was a routine settlement. These are not outliers. According to the **ACCC's National Anti-Scam Centre**, Australians lost more than **\$16.2 million** to payment redirection scams in 2023, with real estate transactions among the top targets.

New data from **Scamwatch** and law enforcement agencies suggests these figures understate the true scale. In Western Australia alone, over **\$500,000 was lost to property-related scams in just the first six months of 2024**, surpassing the total for all of 2023. Nationally, **“buying and selling” scams, which include settlement fraud, led to \$43.2 million in reported losses** last year.

In 2025, PEXA-commissioned research found that **97%** of Australians who've bought a property in the last 12 months or intend to buy in the next 12 months failed to spot dangerous scam markers in property transaction emails, despite most believing they could identify fraud attempts.

Alarming, **around 40%** of respondents said they would transfer funds after receiving a fraudulent settlement email, even among those with high confidence in their ability to identify scams. This highlights a significant gap between perceived ability and actual resilience against fraud.

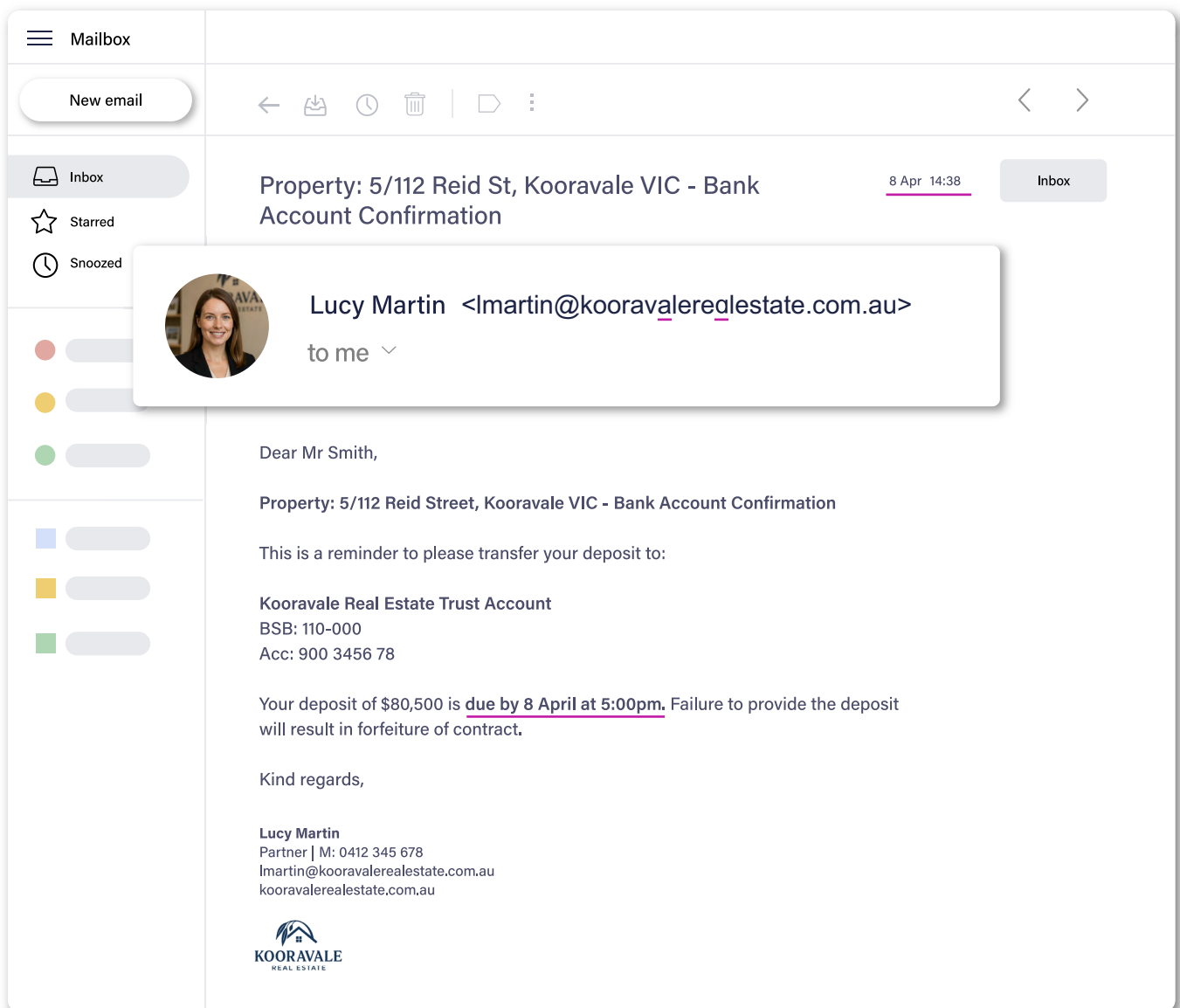
Property transactions involve large sums, short timeframes, and routine reliance on email — the exact scenario scammers like to exploit. Without a strong verification process and public understanding of how these scams work, attackers continue to succeed. Criminals know they don't need to compromise systems, they just need to compromise trust.



# How Property Settlement Scams Work and What to Look Out For

These scams typically unfold through highly convincing yet fraudulent communications. The most common scenario involves email impersonation:

- 1. Email Compromise or Spoofing:** The scammer gains access to or mimics the email account of a party involved in the settlement (such as a conveyancer, solicitor or real estate agent). They may hack an account or create a lookalike email address nearly identical to the legitimate one.
- 2. Timing the Fraud:** The attacker monitors the progress of the property transaction. Just before a payment is due (for example, the deposit or settlement funds), the scammer sends a seemingly authentic email to the buyer (or sometimes the seller or practitioner) with revised bank account details.
- 3. Deceiving the Victim:** The fraudulent email often includes legitimate-looking letterheads, signatures and even attached documents to appear credible. It will urgently request that the upcoming payment be sent to the “new” account, which is actually controlled by the scammer.
- 4. Funds Redirected:** Believing the communication to be genuine, the victim transfers the funds to the provided account. Once the money is sent, the scammers quickly withdraw or launder the funds, making recovery difficult.
- 5. Discovery of the Scam:** The fraud often comes to light only when the real conveyancer or party follows up on the missing payment. By then, the money has vanished, leaving the victim with a significant financial loss.



In the example above, the scammers impersonate the conveyancer with an urgent request to reroute funds. The red flags include the unexpected change of bank details, an urgent tone, and the use of a slightly altered email address (e.g. **@koovalerealestate.com.au** instead of the legitimate **@koovalerealestate.com.au**). Busy and stressed buyers may miss these subtle clues.

## Stay Alert to the Settlement Scam Red Flags

Process steps	People involved
● Buyer's offer is accepted	Buyer Real Estate Agent
▶ ● Buyer's deposit requested by real estate agent	Buyer Real Estate Agent
▶ ● Seller provides source account details to real estate agent	Seller Real Estate Agent
● Deposit received and provided to seller	Seller Real Estate Agent
▶ ● Buyer provides source account details for sending settlement funds	Buyer Conveyancer
▶ ● Seller provides source account details for receiving settlement funds	Seller Conveyancer
● Disbursement of settlement funds	Buyer Seller Conveyancer
● Property settled	Buyer Seller



### Red flags to look out for

- Last minute change of bank details
- Urgency
- Bad email addresses, e.g. subtle misspellings or extra characters
- Unsolicited/unverified requests
- Confirmation of payee warnings

# Staying Safe: How to Protect Yourself

The good news is that there are clear steps everyone can take to dramatically reduce the risk of falling victim to a property scam. Both increased awareness and smart use of technology are key.

The 2025 PEXA-commissioned research shows there is still a significant gap in secure communication practices. Only **1 in 3 buyers** use a secure app for sharing information during settlement, such as PEXA Key. The most common method for sending bank details remains **email**, followed by in-person exchange, both of which can be intercepted. Verification most often occurs via calling a conveyancer or agent on a known number (58% of buyers), while some still reply directly to the original email or SMS, which may be fraudulent.

The research also highlights a behavioural risk: **false confidence**. This phenomenon, known as the Dunning-Kruger effect, occurs when individuals with high confidence in their scam detection skills are actually more likely to fall victim. In the 2025 survey, those with the highest confidence were more likely to transfer funds in a scam scenario (41%) compared to those with low or no confidence (33%). Past victims were also more likely to be scammed again (70% versus 30%). This finding reinforces that awareness alone is not enough, secure verification behaviours must be consistently applied, regardless of experience or self-assessed skill.

**PEXA's security experts and the Australian Cyber Security Centre (ACSC) recommend the following best practices to buyers, sellers and practitioners:**

- **Use secure communication platforms.**  
Wherever possible, avoid relying on regular email for sending or receiving bank details. PEXA offers the PEXA Key app, a free, secure application specifically designed to safely exchange bank account information for settlements<sup>6</sup>. Using such a platform means your account details are encrypted and integrated directly into the PEXA system, removing the opportunity for email interception. (*Notably, PEXA Key's Secure Communication Guarantee even provides reimbursement up to \$2 million if something goes wrong on the platform's side*<sup>7</sup>.) By using secure tools provided by the industry, consumers and practitioners add an extra layer of protection against phishing.
- **Never trust unsolicited email instructions for payments.**  
Always verify any change in payment details through an independent channel. For example, if you receive an email requesting a funds transfer to a different account, call your conveyancer or banker on a known phone number to confirm. Do not use email as a channel for exchanging bank account details as part of settlement.
- **Pay attention to Confirmation of Payee (CoP) warnings.**  
Banks now display a warning if the account name you entered doesn't match the account number. If you see this, stop and call your conveyancer or bank using a trusted number to confirm. CoP adds another opportunity to catch fraud — but it only works if you act on it. The public campaign “Check the Name. Spot the Scam.” reinforces the importance of paying attention to these warnings.

- **Double-check sender details and be alert to red flags.**  
Scammers often create email addresses that look legitimate at a glance. Check the sender's full email address carefully for subtle misspellings or extra characters that don't belong<sup>5</sup>. Be cautious with any message that conveys urgency, secrecy, or pressure to act immediately; these are classic scam warning signs. If an email seems even slightly "off," take a moment to stop and verify the information before taking action.
- **Protect personal data and accounts.**  
Home buyers and sellers should also practice general cyber safety. Avoid clicking on suspicious links or attachments (which could install malware). Do not provide personal or financial information to unfamiliar or unverified requesters via email<sup>8</sup>. Ensure your email account has a strong, unique password and enable two-factor authentication (2FA) to prevent hackers from breaking in. For conveyancers and businesses, maintaining up-to-date security (antivirus software, email spam filters, etc.) is crucial so that your systems don't get compromised in the first place.
- **Act quickly if you suspect a mistake.**  
If you realise you may have sent money to the wrong account or received a fraudulent instruction, contact your bank immediately. Banks can sometimes recall or freeze funds if notified promptly. Then inform your lawyer/conveyancer and report the incident (to the police and via ReportCyber). According to our survey, a majority of Australians said their first call would be to their bank if they were scammed, and this is the right instinct, as time is of the essence in trying to recover funds. Prompt reporting to authorities can also help prevent the scammers from striking again.

## We All Play a Role in Reducing Risk

Keeping property transactions secure is a **shared responsibility**. Each party involved has a role in preventing scams and a stake in the outcome. Below we outline the liability and risk responsibilities of the main parties in a property settlement:

### Home Buyers and Sellers

As the individuals ultimately sending or receiving money, buyers and sellers need to stay vigilant. Their responsibility is to follow the security guidance provided, such as using the recommended secure channels and verifying any payment instructions. Buyers should never hesitate to double-check with their conveyancer or bank if something seems unusual; a simple phone call can prevent catastrophe.

While recent Australian laws now hold banks, telcos, and digital platforms more accountable for preventing and responding to scams, consumers still play a vital role. If a buyer or seller sends money to a scammer's account, recovering those funds can still be difficult and is not guaranteed, although they may have recourse through the Australian Financial Complaints Authority (AFCA).

Therefore, it remains in consumers' best interest to pause and verify at every critical step. Being proactive and cautious is the best defense, and it is far better to delay a settlement slightly than to risk losing one's life savings.

Interestingly, while a large proportion of buyers agree they are part of the security equation, **68% expect at least some reimbursement** from another party if scammed. This expectation persists even though many also believe that scam prevention is a shared responsibility between buyers, banks, real estate agents, conveyancers, and platforms.

*Our research indicates that consumer confidence in the settlement process improves significantly when buyers are made aware of scam risks upfront. Notably, even self-identified “tech-savvy” individuals can be duped if complacent, a reminder that no one is immune without proper precautions.*

## Conveyancers and Solicitors

Property lawyers and conveyancers are on the front lines of these transactions and have professional obligations to safeguard their clients’ interests. They should implement strict processes for verifying client instructions: for instance, many firms now explicitly warn clients they will **never** email bank detail changes, so clients know not to trust such emails. Practitioners must also secure their own systems, using strong passwords, up-to-date security software, and (where available) secure platforms like PEXA for settlements. A compromised conveyancer’s email or practice management system can enable fraud, so their cyber hygiene is critical. Thus, conveyancers should treat cyber safety as integral to their duty of care. Clear communication with clients is key: by educating clients about scams (for example, informing them at the start of the process not to trust emailed bank details), practitioners can shut down the scammers’ window of opportunity.

## Financial Institutions (Banks and Lenders)

Banks and lenders play a pivotal role in detecting and preventing fraud during property transactions. Customers remain responsible for ensuring they send money to the correct account, but banks are now also required to implement safeguards. These include flagging unusually large transfers, checking for mismatched account details, and issuing warnings for high-risk transactions. Many Australian banks already display pop-up alerts when customers transfer funds to a new payee, reminding them of potential scam risks.

**Confirmation of Payee (CoP)** is one of the most important safeguards. This feature alerts customers if the account name entered does not match the account number, creating an additional opportunity to stop fraudulent transfers before they are processed. For CoP to be effective, customers must act on the warning by pausing the transaction and verifying the details with their conveyancer or bank using a trusted number.

Banks may still decline to reimburse funds if a customer authorises a transfer to a scammer. However, under Australia’s new scam prevention laws, they must be able to demonstrate that they took **reasonable steps** to prevent the scam. Victims can lodge complaints through the Australian Financial Complaints Authority (AFCA), which can assess whether the bank met its obligations.

Banks are also responsible for assisting with fraud investigations and, if notified promptly, can sometimes freeze or recover funds before they are moved beyond reach. This reinforces the need for immediate contact with the bank if a scam is suspected.

**2025 research insight:** In the national survey, **41 percent** of respondents said their first action if they suspected a scam would be to contact their bank, compared to 22 percent who would contact a conveyancer and 16 percent who would contact a real estate agent. This underlines the central role of financial institutions in both prevention and immediate response.

Beyond transactional monitoring and CoP, banks contribute through public education, issuing scam alerts, and running awareness campaigns. Many also participate in industry initiatives such as the National Anti-Scam Centre, working with government and other stakeholders to disrupt scam operations. Their role is therefore both **protective** – preventing fraud where possible – and **reactive**, responding rapidly when incidents occur.

## PEXA and Digital Platforms

As the trusted digital settlement platform for conveyancers and financial institutions, PEXA plays an important role to protect the integrity of property transactions. **Security is embedded into the platform's design and operations**, from enforcing multi-factor authentication for all users to maintaining strong system protections against fraud.

The launch of **PEXA Key**, backed by a **\$2 million Secure Communication Guarantee**, was a direct response to the growing threat of email-based payment redirection e.g. email phishing scams. This secure app provides a safe, encrypted channel for exchanging bank details, removing the vulnerabilities of standard email.

The 2025 research shows that only **around 22 percent of those who bought a property in the last 12 months or are intending to buy in the next 12 months** place primary responsibility for scam prevention on digital settlement platforms. This presents both a **communications challenge** and an **opportunity**. By positioning PEXA's secure tools, such as PEXA Key, as **essential components of scam prevention**, there is potential to shift buyer perceptions and increase adoption of secure practices.

PEXA also invests in **education and training** for practitioners, encouraging adoption of its secure features and reinforcing the principle of **shared responsibility** for fraud prevention. When all parties use the platform as intended, including pre-verifying account details and avoiding email for sensitive information, the risk of settlement fraud is **significantly reduced across the network**.

## Transaction responsibilities

Buyer/Seller	Practitioners (Conveyancers, lawyers)	Bank	Platform
<ul style="list-style-type: none"> <li>• Verify payment information</li> <li>• Use secure channels</li> <li>• Use strong passwords and two factor authentication</li> </ul>	<ul style="list-style-type: none"> <li>• Clear communication with clients</li> <li>• Use secure channels, e.g. onboarding clients to a secure app like PEXA Key for the transaction</li> <li>• Use strong passwords and two factor authentication</li> <li>• Consider pre-establishing processes to address scam risks, e.g. agreeing a verbal password with clients</li> </ul>	<ul style="list-style-type: none"> <li>• Monitor secure channels</li> <li>• Issue warnings for high risk transactions</li> <li>• Checking for mismatched account details</li> </ul>	<ul style="list-style-type: none"> <li>• Monitor secure channels</li> <li>• Strong cybersecurity safeguards embedded into the platform</li> <li>• Supporting practitioners with education and training on fraud prevention</li> </ul>

## The Scams Prevention Framework

### Understanding how it will apply to settlement scams

The Government has adopted a phased approach to regulation of scam activity. The first phase was the implementation of the ACCC's National Anti-Scam Centre. The Scams Prevention Framework, which became law in February this year, is the second phase. The Framework adopts a whole of ecosystem approach to provide protection against scams for individuals, as well as small businesses.

Under the Framework, a scam includes an attempt to deceive individuals (or small businesses) into making payments using a designated "regulated service". While services have not yet been designated, the Government has stated that the first services to be subject to the regime will include those provided by banks. Therefore, from the time it first takes effect, the Scams Prevention Framework will apply to property settlement scams.

The Framework has **six overarching principles**, including:

- 1. Prevention:** reasonable steps must be taken to prevent scams - for example, banks could warn customers about scam trends.
- 2. Detection:** reasonable steps must be taken to detect scams – for example, banks could use algorithms to detect suspicious activity.
- 3. Disruption:** reasonable steps must be taken to disrupt suspected scam activities to protect consumers and small business – for example, banks could suspend scam accounts.
- 4. Responsiveness:** regulated entities must allow consumers and small business to report scams and must have in place an internal dispute resolution mechanism for resolving complaints about scams.

The **other two** overarching principles require the implementation of appropriate governance regimes and reporting.

In support of the overarching principles in the Framework, mandatory industry codes will be implemented to impose minimum standard on a sector by sector basis, and will be tailored for the specific circumstances of the relevant sector.

PEXA supports the Framework, which builds on the important work that has already been done to address property settlements scams. The Framework reflects that combating such scams is a shared responsibility that requires a “hands on” approach. Although PEXA will not be directly regulated under the Framework’s banking code, we look forward to working with the banking sector and ASIC, which will be the responsible regulator, in the implementation of the Framework regime.

# Conclusion

Property settlement scams are a serious threat, but they can be thwarted through awareness, vigilance and collaboration across the industry.

As we mark Scam Awareness Week 2025, the core advice bears repeating: **Stop. Check. Protect.** Take a moment to **stop** and question anything unusual; **double-check** requests through trusted channels; and use every **protection** available, from secure apps, strong authentication, to paying attention to Confirmation of Payee (CoP) warnings.

CoP adds a crucial final check — but it only works if you act on it. When you see a CoP warning, stop, check, and confirm payment details through a trusted channel before proceeding.

Together, we can keep the property ownership journey safe and positive. Stay alert, stay informed, and outsmart the scammers at every turn.

## About the Consumer Research

The PEXA Research on Property Settlement Scam Awareness was conducted by Nature on behalf of PEXA. It was in market in July 2025. There were 1,030 respondents nationally, comprising 474 respondents that bought a property in the last year and 556 respondents intending to buy property in the next 12 months.

## Additional Information

<b>Site Name &amp; Link</b>	<b>Description</b>
<a href="#"><u>Scamwatch (ACCC)</u></a>	Official government scam awareness website run by the ACCC. Provides up-to-date information on common scams and how to get help if you've been impacted, and allows consumers to report scams online.
<a href="#"><u>National AntiScam Centre (NASC)</u></a>	ACCC-run initiative bringing together government, law enforcement and industry experts to disrupt scams before they reach consumers. Analyses scam trends and shares data to raise public awareness about spotting and avoiding scams.
<a href="#"><u>Australian Cyber Security Centre (ACSC)</u></a>	Government cyber security hub that monitors online threats and provides guidance on protecting yourself (and your business) online, plus advice on responding to cyber security incidents. The ACSC also hosts the <b>ReportCyber</b> portal for reporting cybercrimes.
<a href="#"><u>ReportCyber (ACSC)</u></a>	Australia's official online cybercrime reporting portal (operated by the ACSC). Allows victims to report scams, fraud, and cyber incidents directly to authorities. Reports help law enforcement and the National Anti-Scam Centre identify and disrupt criminal operations.
<a href="#"><u>IDCARE</u></a>	Australia's national identity and cyber support service for victims of identity theft or data breaches. Provides free specialist advice and counseling to help individuals secure accounts and recover after a scam incident.
<a href="#"><u>PEXA Key, Secure Settlement App</u></a>	A free, secure mobile app by PEXA for property buyers and sellers to safely exchange bank account details during settlement. Protects against email payment redirection scams e.g. email phishing scams, by encrypting and transmitting account information through PEXA's secure platform (backed by a \$2 million Secure Communication Guarantee).