Scam Prevention and Awareness Live Webinar – Transcript

TITLE SLIDE – Scam prevention and awareness session

SPEAKER 1 – Christina

Introduction

EXPLANATION

Welcome and thanks for joining our scam awareness and prevention virtual session.

Hi, I'm Christina, I'm here today with my colleague Sarah, and we're both fraud and scam education and awareness managers at the Westpac Group.

We've both worked for the group for over 15 years and we're passionate about helping our community.

Today we're here to help increase your scam prevention knowledge and empower you to avoid scams.

The more we know about scams, the warning signs, scammers' tactics...and the more we share this with family and friends...the better we'll be able to help protect each other from scammers and reduce their impact on the community.

Unfortunately, it's a conversation that needs to be had indefinitely, as scammers are always looking for new and creative ways to steal our money and information.

"Before we begin today, I would like to acknowledge the traditional owners of the land on which we meet and pay my respects to elders both past, present and emerging.
I also acknowledge and pay respects to those here today who identify as being Aboriginal and Torres Strait Islander and recognise the diversity of Indigenous peoples, countries, and culture in Australia.

We acknowledge our role in supporting an inclusive and diverse nation where all of our cultural backgrounds are recognised and respected."

To get us started, it's important for us to understand the difference between a fraud and a scam.

Fraud is when the customer did not authorise the transaction and/or method of loss. An example of fraud could be that your credit card is lost or stolen and then used by the fraudster.

The volume of fraud that runs through our banking platforms in comparison to legitimate transactions is minimal. However, the increasing number of customers who are tricked into sending money to criminals is concerning.

A Scam is when the customer willingly participated in the transaction but has been misled regarding the benefit or purpose. They can be more challenging to detect as they are disguised as genuine transactions.

Scammers will often gain your trust quickly and have you believing that the bank, your family, and friends are the ones to beware of. They'll coach you in what to say to the bank, in an attempt disguise the transactions as genuine, making it very challenging for us to help and stop the financial loss before it happens.

Scammers will also try to isolate you and tell you not to talk to family and friends, because they know if you do, they might stop you from speaking to the scammer.

We hear a lot during these types sessions and through discussions with the community that 'I won't fall for a scam', and while this may be true for some, it's important to remember that scammers are also very smart and convincing and are always working on new ways to target us in the hope we'll believe them.

With this in mind let's look at the impact of scams on everyday Aussies.

Scammers are very active in our communities, so if you've ever been impacted by a scam or know someone who has, you're not alone.

In 2020 Australians lost nearly $851 million dollars to a variety of scams and this number is trending up, not down. All scam types have reported increases in both numbers and the amount of money lost.

It's also known that this number is significantly underestimated as it only includes scams that have been reported to Australian Government agencies.

The numbers do not include:

- People who don't know they're being scammed.
- People who have been emotionally impacted and decided not to report.
- And People who are unaware of when, how or where to report scams.

ASK

Living in Australia, what does this mean for you?

It means that for every person impacted by a scam, they stand to lose on average $7677.

Some victims have lost less and some a lot more; amounts in the hundreds of thousands have been reported, in some cases millions.

It's not always just money that is lost; it can also be personal information that scammers use for their gain, for example applying for credit in your name.

ASK

So where does this scam money go?

Well, It's not to anything good.

Stolen funds get broken up into various transactions or purchases by money mules, and could fund organised crime, individual criminals, or terrorist groups, in Australia or overseas.

The statistics you'll see today, have been sourced from the ACCC and other Westpac partners, including Scamwatch and IDCARE.

At Westpac we have support teams who work around the clock to detect suspicious behaviour and keep you and your money safe.

Westpac has some very sophisticated technology to support you. In fact, our fraud and scam detection is the best in the market.

We detect and confirm transactions against your banking activities and alert you when something isn't right. We may contact you or send you a code if we see unusual activity for Online Banking or payments, this is to confirm it is you completing the transaction and help protect your money.

That is why it's vital not to share these codes with anyone and that all your contact details with the bank are up to date.

If you believe you've been impacted by a scam, contact us immediately so we can attempt to recover any funds. Unfortunately, in most cases locating the money and recovery is very difficult as the money may

have been moved offshore or taken out in cash. It's also worth us noting the difference between a recovery and a refund.

A recovery is not a refund - it's when we attempt to find the money you willingly authorised and transferred. It's a request that we send to the individual/scammer or their bank to return the money to you; but if the money is gone it can be too late to recover.

Our branch staff are also there to help and protect you so please get in touch with them and raise any questions or concerns you have; and be honest with us, to help us protect your money.

In addition to technology and alerts we also help through education and awareness initiatives, like today's presentation, and there's loads of helpful information on our website.

Another key part of protection is partnering with government initiatives. Westpac partners with several Government initiatives to increase scam awareness for all Australians. For example, the ACCC, law enforcement, IDCARE and many more.

AGENDA

EXPLANATION

In today's presentation we'll cover:

- The types of Scams and how you may be targeted.
- We'll explore different types of scams, using case studies based on real life scenarios. This will help you identify the possible warning signs for these scams.
- And We'll direct you to the available resources that you can access for support and reporting.

TYPES OF SCAMS OVERVIEW

EXPLANATION

Scammers have many tactics that they use to try and convince you into giving them your money and/or your personal information. They cast a wide net and hope to scam as many people as possible to maximise their gains.

Here is a list of different scam types. Today we'll go over some of the most common scams impacting our customers and communities.

Not all the scam types we cover today will be apply to you. But as we go through each one, consider the other people in your life who may be vulnerable to these scams. Help them by sharing what you learn today and already know.

SCAMS VIA THE PHONE

EXPLANATION

Currently, the most popular way for scammers to target you is via the phone.

More than half of all reported scams start via the phone. This could be a home, mobile or business phone number, even if you have a private number or are registered on the do not call list, unfortunately it doesn't stop scammers.

Usually, these calls are from someone pretending to be a reputable business or company that you're familiar with for example your bank, telco, internet provider, a company questioning transactions with you, like online shopping providers or even a government agency like the ATO.

During these calls they may ask you for personal information, demand you pay money or in some cases they'll state they're going to pay you money in the form of a refund or deposit for your help in return.

Listen out for the potential warning signs that it could be a scam call:

- Someone is applying pressure for you to do something immediately, for example pay a bill or transfer money.
- There's a threat or penalty for not completing their actions, for example arrest or prosecution.
- You're asked to download software on your computer or mobile device.
- Or you're asked to sign into online banking.

Never follow instructions from an unsolicited caller, always validate requests by calling the genuine company on their publicly listed number, and don't call back using the number provided by the unsolicited caller.

Always take time to pause and consider if the call is genuine and would this company or provider contact me to request this type of action. You Should double check with a family member, a friend, or the bank before you take any action.

EXPLANATION

A phone scam that's increasing at an alarming rate is one we call a remote access scam. It's called this as it involves you giving another party access to your computer or mobile device remotely, by downloading software. Let's look at an example.

- Dani received a call from someone pretending to be a representative from her phone company, it's a company she deals with all the time.
- The caller advised that they needed her help to catch a fraudster and they could see fraudsters already had access to Dani's computer. Dani was directed not to tell anyone, including her bank as it would jeopardise the investigation
- Dani was then instructed to download software, She followed the instructions and accepted all screen prompts that were presented. Not understanding this was giving the caller full access to her computer.
- Dani was asked to sign into online banking and confirm her account number to receive a deposit which would allow them to catch the fraudster.
- The caller then asked Dani to check her balance had increased by $10,000 from a deposit the caller had placed in her account. The screen disappeared and reappeared, and the caller advised they were hot on the path to the fraudster.
- The caller requested the $10,000 deposit be withdrawn in cash and returned to the internet provider via a wire transfer.

The software that Dani had installed on her computer is a form of 'remote access software'. This allowed the Scammer to take full control of her computer, including viewing her browser when she signed into Online Banking.

The scammer then performed a funds transfer from her available credit card balance into her everyday transaction account. This made it look like she'd received additional money via a deposit when the money was her own. She then withdrew the cash and sent it to the scammers.

This type of scam has many variations, although several things remain the same:

- They start with contact usually via the phone, where the caller is someone pretending to be from a reputable company or a company you're familiar with.
- You're asked to download software (to access your computer).
- It may look like you receive a deposit of money or a larger than expected refund and are instructed to transfer it back via online banking or a different method.
  Remember in these cases the money is your money, not the scammers.
- The caller may become aggressive if you don't comply with their requests or ask that you remain on the phone when you go to the bank so they can instruct you what to do and say.
- You may be prompted to call a reputable company from a popup message to help with technical support – please note tech companies like Microsoft advise they don't include numbers for you to call via a popup message.

EXPLANATION

Common ways to spot this type of scam.

- You receive an unsolicited call from someone pretending to be from a reputable company.
- A scammer may tell you not to tell anyone or they may coach you on what to say to the bank.
- On the call you might be asked or instructed to download software or application like Team viewer, Anydesk to allow remote access to your computer or device.
- You're asked to pay money via an unusual payment method – money transfer agent, gift cards, crypto currency, cash rather than online banking.
- Caller is aggressive, pushy, or demanding.
- You receive a popup with a contact number for tech support.

ASK

To protect yourself from Remote access scams

- Don't download software that allows others to control your devices or follow instructions from an unsolicited call.
- Before completing any actions, confirm with the company directly using their publicly sourced contact information - not what is provided by the caller.
- Be aware of the caller's behaviour, consider would this company ask me to do this?
- Hang up at any point where the callers behaviour doesn't seem right and talk to trusted friends and family for a second opinion before you take any action.

Remember Never disclosure your security codes, like your Westpac Protect SMS code for online banking transactions to anyone. This is how we keep you safe and know it's you making the transaction. It's ok to hang up and seek help.

Someone who has remote access to your computer or device has access to everything, can see everything and they can also download other types of Malicious software.

If you suspect this has happened to you, turn off your computer or device. Don't use this device until it's been professionally cleaned by a reputable technician and contact your bank immediately.

EXPLANATION

Another common phone scam is a threat and penalty scam, Let's take a look at a case study involving this type of scam:

- Jane received a call from someone pretending to be from the Australian Taxation Office.
- She was told she had a tax debt and if she didn't pay it immediately, she would be arrested and go to jail.
- Jane was instructed to purchase crypto currency to pay the debt.

The caller was very persistent, and the threat sounded legitimate. Jane didn't want to be arrested and was scared, so she followed the caller's instructions and paid the money.

EXPLANATION

To spot this type of scam, again, be cautious and suspicious of unsolicited calls in which the caller requires urgent action or there are any payment requests in crypto currency, gift cards or any other unusual payment method.
Scammers may also request remote access to your device to help you complete these types of payments.

EXPLANATION

To protect yourself from threat and penalty scams

- Be cautious of calls from unknown numbers, private or international numbers that hang up before you can answer the call. Don't call back just ignore them.
- Hang up the phone and call the company directly using their publicly listed contact information. Don't use the number provided by the caller.
- Don't be pressured by a caller, always Stop, Think and Check whether the story sounds genuine. Use your instincts if it doesn't feel right or is unexpected - it is ok to hang up.
- Be wary of requests to pay via unusual payment methods like gift cards, crypto currency or via overseas transfers.

Let's hand over to Sarah to take us through more scam types.

TITLE SLIDE - ONLINE – Think before you click!

SPEAKER 2 – Sarah

New Speaker starts to speak.

EXPLANATION

We've looked at the types of Scams you may get via the phone; now let's consider some online or computer scams.

Online Scams are the second most successful way scammers target you, with more than 30% of all scams occurring online via email, browsing the internet or social networks.

As you can see online scams can present in so many.

We'll look at some of the most common online scams starting with a phishing email.

Here's an example of a phishing email (spelt ph), in this example, scammers altered a Westpac marketing email to make their request seem more legitimate, we've highlighted a couple of the tips to help you spot this type of scam.

- You can see it asks the user to click on the link to reactivate or verify their account.
- There are no salutations, and there is a sense of urgency to complete the action.

We'll never ask you to confirm transactions, personal details or unlock your banking via a link sent through an email or SMS text message, nor will we ever send you a link that takes you directly to sign into online banking.

If you get an email with a link and you're unsure if it's genuine, you can hover your mouse over the link without clinking on it to display the web address or URL this will take you to.

The example on screen is not a genuine Westpac link and it's hard to identify where it would take you, therefore it's best not to click the link.

If you're unsure, always sign into Westpac by visiting our website directly or using our mobile banking app.

Westpac emails that look like this should be sent to hoax@westpac.com.au, don't open any links and delete the email or SMS text message immediately after you've forwarded it to us.
If you ever click on a suspicious link, please turn off your computer or device and contact your bank immediately.

False Billing

False billing is another way a scammer may try to get your money or personal information.

Like the previous example, false billing is when scammers pretend to be from organisations you know and use their templates to convince you it's a legitimate bill or invoice. In some cases, malicious software may be installed on your device by clicking a link or opening an attachment.

Another slightly different version is a sophisticated scam called a Business Email Compromise or BEC scam.
In these scenarios' payment details are modified to those of the scammers account details and added to bills, invoices, or other payment requests usually for large payments like a house deposit or large business purchase.

To spot this type of scam, consider if.

- You have any accounts with that provider,
- Have the payment details changed from previous bills?

- Is this a one-off large payment?
- Did the payment instructions come from an email?

To protect yourself against false billing and BEC scams:

- Always confirm all new or changed account details on any large emailed invoices, verbally with the provider directly. Don't use the contact information in the email or invoice as the email account may have been compromised by a scammer.
- Use official online websites and apps to make payments or contact the provider directly on a publicly sourced number.
- Ensure you have appropriate security software for your needs, and it's kept up to date. Encrypt or password protect confidential emails.

Another common online scam we'll explore is investment scams. In the last 3 years Aussies lost the most money to this scam. Let's talk through this example.

- Steve is a 65-year-old retiree, he received an unexpected call about an investment opportunity.
- The caller sounded very professional and knowledgeable on investment matters. They answered all of Steve's questions and followed up with a call from a 'senior advisor'.
- Steve decided to explore this new investment opportunity and over the next 12 months, Steve made several transfers starting with $10k.
- He was referred to a very professional looking website and set up an online account, which showed his money increasing in value. He was even able to withdraw some money which increased his confidence that the investment was genuine, so he invested more money, to a total of $200k

Steve realised this was a scam when the website went offline, and he couldn't access his account or contact the offshore group by phone.

Steve found out that it was a fake company and wasn't registered with the Australian Securities Investment Commission (ASIC). He was too embarrassed to tell anyone or report it. Sadly, none of Steve's money was ever recovered.

EXPLANATION

Some ways you can spot an investment scam:

- You receive unsolicited contact via phone, email, social media, or an online ad.
- You're promised high returns on investments over a short period of time.
- There is Pressure or intimidation to make financial decisions on the spot.
- The opportunity is backed by fake celebrity endorsements.
- Investment opportunities in crypto currency where a broker or company takes control of the investing for you.
- Your money is going overseas, or transfers are made payable to different names and account numbers for the same investment.
- You're told not to tell anyone or are coached on what to say to the bank.

- You're offered training and assistance with your investment through providing remote access to your device.

EXPLANATION

To protect yourself from Investment scams consider

- If it seems too good to be true, it probably is! Be suspicious of investment opportunities that promise a high return with little or no risk
- Don't give your personal or financial details to unsolicited callers or reply to emails, SMS or online ads offering financial advice or investment opportunities.
- Always contact the company or organisation directly using publicly sourced phone numbers, not what's provided via an email, online ad or popup message.
- Discuss opportunities with your financial advisor/ planner or Accountant (independent from the caller).
- Always do thorough research on investment companies, advisors, or apps. Any business or person that offers or advises you about financial products must hold an Australian Financial Services (AFS) licence. Always Check financial advisors are registered on the ASIC website. For more on this, go to www.moneysmart.gov.au
- Don't let anyone pressure you into making decisions about your money - always get a trusted second opinion from a licenced professional.
- Install and keep security software up to date on all devices. Don't open or use any links in suspicious emails, texts or pop-up messages.

Remember if it seems too good to be true it probably is!

EXPLANATION ON ROMANCE SCAMS

Another common online scam is romance scams.

Romance and relationships scams are heart breaking, each year they cost Australian's millions of dollars. Let's look at an example now.

Andrew met Maureen online - she lives overseas.

- Although they've never met in person, within 4 months they're engaged.
- Maureen says she was involved in a serious accident and needs money for her medical bills.
- Andrew completed 10 transfers totalling $320k.
- Once Maureen knew she had taken all of Andrew's money she ceased all contact with him.

Andrew realised something didn't feel right once Maureen ceased contact.

He spoke to his bank to get his money back, but Maureen had already withdrawn all the money and it couldn't be recovered.

It's always important to consider that a romantic connection formed online could be a scam, even if you speak to them on the phone all the time.

EXPLANATION

Some ways you can spot a romance scam:

- The scammers are quick to change "chat" platforms from a Dating site to social media or whatsapp. This is to avoid you being suspicious of their false profiles and to stop you from reporting them.

- You've never met in person; and they provide excuses as to why they cannot video chat but may encourage you to share your video.
- They confess love quickly and propose before meeting in person.
- They ask for money with an elaborate story – an accident, family issues or are stuck in another country.
- These scammers isolate you from your family and friends with frequent contact, they build trust and explain that no one will understand your connection.

EXPLANATION

To protect yourself from relationship scams:

- Don't send money or provide your personal details to someone you have only interacted with online or via the phone.
- Be cautious of unknown "friends" when using online services. Not everyone is who they say they are online.
- Be wary of what you share. Also be aware of friends that may have had their social media account compromised, the scammer will set up a duplicate profile and start chatting to you - you'll think it's your friend when it's actually a scammer.
- Do an online search of your admirer or their image to see if they are who they say they are. Often, you'll discover the same photo used with different names attached to multiple profiles.
- Watch out for admirers who want to contact you outside the dating/social media website after just a few interactions.

Romance and friendship scams can happen to anyone, especially at times when you may feel lonely or vulnerable. It's important to try and remove emotion from your decision making when money is involved, no matter how caring or persistent your new partner is. Remember scammers do this for a living.

If you ever have any doubts, turn off your device and give yourself time to consider the situation and talk to family and friends, even if your new partner has convinced you not to.

Now lets take a look at how you may be targeted -At your door.

DEBRIEF

Scammers have moved on from traditional door to door scams, targeting us using technology, though some may happen at your front door.

Here are some examples of how you may be targeted at your door:

- You could have a scammer impersonating a charity or tradesperson.
- You could receive lottery or a scratchie in your letter box, stating you've won money or a holiday.
- You could have your mail taken from your letter box and then your identity stolen.
- Scammers may even collect money from you in person, often in conjunction with another scam types.

Be very cautious of people who come to your door. There is an increase in impersonation scams, and they can be quite sophisticated. For example getting a call from someone pretending to be from the

bank saying your card has been compromised and sending people dressed in a bank uniform to pick up your card and PIN from your home or acting as a courier to collect gift cards or cash.

Please be safe, don't let anyone into your home that you don't know and never give your cards and PINS to anyone.

Some overall -Scam Warning Signs

EXPLAIN

Throughout today's examples you've most likely picked up on some of the scam warning signs.

We want you to feel confident and knowledgeable that if you see or hear any of these warning signs, you'll cease communication and report it right away.

The warning signs are:

- You're asked to share your passwords, security code or SMS code with anyone, this includes your family and friends.
- If an offer claims that you can't lose, has no risk, or simply seems too good to be true.
- You receive unsolicited contact via phone, email, SMS or a popup message, with pressure or intimidation to complete an action on the spot.
- Your personal information is requested.
- Out of the blue requests to pay or transfer money, .
- The contact person's details are vague / confusing / or lack return contact information.
- You're told not to tell anyone or are coached on what to say if asked.
- Your gut instincts tell you something doesn't feel right.

If in doubt, hang up the phone, delete the emails, shut the door, and bin the letter.

If you believe you or someone you know may have been impacted by a scam, it's important you advise your bank, report it and talk about it.
It could be your insight and conversation that stops you or someone you know losing money.

EXPLANATION

I think after today it's clear we can all be impacted by scams and we all want to stop the scammers. Here are some tips to help protect yourself and others from scams.

1. **Consider if the request genuine. Always research who you're dealing with and/or get a trusted second opinion.** –take the time to consider, research and talk about requests before you act.
   Urgency is a tactic used by scammers to trick you into doing what they want.
   Ask yourself questions:
   Is the company registered with ASIC as a registered business?
   Would they contact me in this way about this topic?
   Does this sound right? Is it too good to be true?
   Wouldn't everyone be wealthy and investing if this deal was real?
   Contact providers directly using a publicly listed phone number to check if the offer or request is genuine
   Google image search photos of potential new friendships.

2. **Keep Security software up to date on all devices. Don't open suspicious texts pop-up windows or emails - delete** – always delete them! Don't use contact information within suspicious emails or pop ups, don't click on any links.

3. **Keep your personal/business details secure including passwords and security codes**, put a lock on your mailbox, and shred to destroy any old bills, letters, or documents with any personal information.
   Never share your passwords and security codes with anyone; these are the banks way of protecting you and your money.
   Limit information you share on social media like birth dates, maiden names and don't complete those get to know you quizzes. Scammers use socials to get information about you to personalise scam attempts and even hack your passwords.

4. **Use unique passwords for all online accounts and change frequently** –have complex and unique passwords for every service you use – especially your online banking and email accounts, please don't share any of these details with anyone including loved ones. If available turn on and use Multi factor authentication to prevent unauthorised access.

5. **Beware of requests for your details and or money; this includes unusual payments and deposits** You should be on high alert of payment requests via an unusual method like a wire transfer, pre-loaded credit card, iTunes gift cards or digital currency bitcoin, these are nearly always a scam. Only provide your account details to those you trust, and don't agree to transfer money or goods on behalf of someone else.

6. **Be open with the bank regarding your transactions. The bank needs all the information to protect you and your money**
   scammers often provide instructions and coach you on what to say to the bank so we're not suspicious of the scam. For example you're told to tell the bank it's for another purpose such as renovations or car purchases, talk to your bank and please be honest - we're here to help keep you safe

7. **Regularly visit your banks' security page.** Scams are always evolving, so staying up to date helps you avoid being impacted by new scams.

8. **Never give a stranger or unsolicited caller remote access to your computer or device** Providing anyone with remote access to your device is like giving them your front door keys and alarm codes, allowing them to access everything, including your money and personal information. Aussies lost $8.4 m to this scam alone in 2020 and it's one of the highest reported scams today.

EXPLANATION

Help and support

We've spoken about lots of different scams, but where do you go for help if you've been impacted?

We recommend chatting to someone from your bank or a trusted family member or friend.

Check out our handy be safe and secure guide available from our website.

Westpac have partnered with IDCARE who are an Australian not for profit organisation. They offer a range of support services for those impacted by scams, including helping you re-establish your identity after its been stolen.

There are also several counselling services available: for example, Lifeline, Beyond Blue and Financial Counselling Australia.

Remember scammers will try to isolate you from your support networks and tell you not to share what you're doing with anyone.

Please keep talking about different scams so that others know they exist, have open conversations with family and friends about any unusual calls emails or new relationships and listen out for scam warning signs.

Where to Report a Scam

EXPLANATION

We know many people impacted by scams don't report them and the numbers of Australians impacted is underestimated.

If you get caught up in what you think is a scam, been targeted or approached by a scammer, always contact your bank, and report it. You can also report scams to Scamwatch or the Australian Cyber Security Centre (if it is a cybercrime)

These reported cybercrimes filter back into law enforcement and help our government keep track of the impact of these crimes on our communities.

You can also report directly to organisation being impersonated, so they can help stop the scammers too.

Stay Safe

EXPLANATION

Thanks for joining us to learn more about scam prevention.

Please start conversations with your family and friends about what you've learnt.

The information you share with a loved one or friend could stop them falling for a scam in the future.

If you're ever unsure, please get in touch with us.
For more information about scams visit our Westpac security hub.

Thanks