Australian Government
AUSTRAC

Fintel Alliance

Australian Government
Services Australia

PREVENTING THE **EXPLOITATION** OF EMERGENCY & DISASTER SUPPORT PAYMENTS

FINANCIAL CRIME GUIDE DECEMBER 2021

COPYRIGHT

ATTRIBUTION

ACKNOWLEDGMENTS

This financial crime guide was developed by the Fintel Alliance, a private-public partnership led by AUSTRAC.

Thank you to all of our partners who contributed to this financial crime guide.

CONTENTS

HOW TO USE THIS FINANCIAL CRIME GUIDE

This financial crime guide provides indicators to assist the financial services sector to detect and report suspicious transactions related to potential fraud and the misuse of taxpayer funds through Services Australia administered emergency and disaster payments.

The information your business holds can help AUSTRAC, Services Australia and law enforcement partners to identify, disrupt and prevent fraud against support payments delivered by Services Australia. This misuse of taxpayer funds denies people in genuine need access to money to meet their most basic needs such as food, shelter and other necessities.

Where suspected offending is identified, financial services businesses must consider their anti-money laundering and counter-terrorism financing (AML/CTF) obligations and enhanced customer due diligence program. When you form a suspicion about a customer, you should also consider carrying out extra checks on the customer's identification, collecting and verifying additional information.

No single financial indicator will be definitive in determining if an individual is committing emergency or disaster payment fraud. Financial services businesses should use a combination of the indicators in this report combined with knowledge of your business to monitor, mitigate and manage suspicious activity.

ABOUT FINANCIAL CRIME GUIDES

Financial crime guides provide detailed information about the financial indicators of different crime types. They include case studies that can be used to help identify if this type of offending could be occurring.

They are developed in partnership with AUSTRAC's Fintel Alliance members, relevant government agencies, and industry partners.

SUBMITTING AN SMR

If you identify indicators of potential fraudulent activity involving emergency and disaster support payments, please submit a suspicious matter report (SMR) to AUSTRAC. To assist AUSTRAC in targeting this activity, include crime type key words and a description in your report on emergency and disaster support payments.

INTRODUCTION

The COVID-19 pandemic has created a level of community need not seen in 100 years. Combined with other emergency events, such as natural disasters, there has been an increasing demand for emergency and disaster payments from Australians in impacted communities.

In disaster relief and emergency situations, it is essential that government services and support reach those in need quickly.

High profile relief programs are often an attractive target for those seeking financial gain, with fraud carried out by opportunistic individuals and organised crime syndicates.

The exploitation of emergency payments is constantly changing, as criminals frequently find new ways to operate to avoid detection and continue offending.

A RAPID RESPONSE

The Government responds quickly to disasters by rapidly implementing relief and recovery measures to support those affected.

Unfortunately, a small number of individuals and groups try to access payments they are not entitled to by committing fraud.

ABOUT SERVICES AUSTRALIA

Services Australia is responsible for the delivery of social, health, child support and other government payments and services in Australia.

In 2020-21, Services Australia delivered $230.1 billion in social support payments, including approximately $21.5 billion in emergency and disaster payments to people affected by COVID-19, floods, fires and cyclones.

The majority of people claiming disaster assistance are in genuine need of urgent help. Unfortunately, a small number of individuals and groups try to get payments they are not entitled to by committing fraud, often enabled by stealing the identities of vulnerable Australians.

ABOUT THE FINTEL ALLIANCE

The Fintel Alliance is a public-private partnership led by AUSTRAC that brings together government, law enforcement, private sector and academic organisations who work together to:

- support law enforcement investigations into serious crime and national security matters
- increase the resilience of the financial sector to prevent criminal exploitation
- protect the community from criminal exploitation.

The Fintel Alliance partners include businesses from the financial services, remittance and gaming industries as well as law enforcement and security agencies within Australia and overseas.

IMPORTANCE OF PARTNERSHIPS

The Fintel Alliance recognises fraud against emergency and disaster payments in Australia as a serious risk and partners with financial services businesses to target, disrupt and deter offending to protect the community.

Financial services businesses play an important role in combating emergency and disaster payment fraud. Through profiling and transaction monitoring, your business can target, detect and disrupt financial transactions associated with this fraud.

SUPPORT WHERE NEEDED

During or following an emergency or disaster, including health emergencies, the Australian Government provides multiple forms of assistance such as support and disaster payments. These payments are intended to help and support those in the community who need it the most.

The most recent emergency support declared was for ongoing payments to individuals and families during the coronavirus (COVID-19) health emergency. Services Australia delivers a range of payments and support for people affected by COVID-19 in situations where different eligibility applies. Lump-sum and recurring payments were available for those unable to work due to COVID-19 public health orders, or who were unable to earn an income due to compulsory self-isolation or quarantine. These payments also extend to those caring for someone in self-isolation or quarantine due to COVID-19 and in some instances, those already in receipt of income support from Services Australia.

Support following a major disaster (such as bushfires, cyclones and flooding) normally includes the:

- Australian Government Disaster Recovery Payment – a lump sum payment that assists those who have had their principal place of residence significantly damaged, were seriously injured or have an immediate family member who has died or is missing due to a disaster
- Disaster Recovery Allowance – a short-term payment that assists those who have lost income due to a disaster. This type of disaster support is payable after the Minister responsible for emergency management and disaster assistance makes a determination.

Payment amounts and eligibility rules vary across states, emergencies and disasters. Up-to-date information regarding assistance is available in the Help in an emergency section on the Services Australia website.

WHY DOES FRAUD AGAINST GOVERNMENT SUPPORT PROGRAMS HURT THE COMMUNITY?

Fraud against Australian Government support programs hurts the whole community. It diverts taxpayer funds and resources away from people who are facing hardship, and hinders the government's ability to deliver services to those in need. We all have a role to play in ensuring support is available for those Australians that need it during difficult times.

FRAUD METHODOLOGY

Sophisticated fraud networks or individuals acting alone can conduct fraud against emergency and disaster payments.

These fraud networks recruit willing participants to falsely claim payments or compromise unknowing victims' identity data to create and control fake customer profiles. Larger organised crime networks do not limit their fraud to Services Australia programs, but target Commonwealth and State government support schemes and financial institutions.

Less sophisticated fraud usually involves individuals manipulating their personal circumstances to obtain financial advantage during or after a disaster or emergency. They achieve this by using falsified documents or deception to prove their payment eligibility. This type of fraud is typically opportunistic, but often involves repeat offenders. It may spread via 'word of mouth' in geographic communities, or community groups.

Fraud methodologies for these payments fall into three categories: qualification misrepresentation, organised cluster fraud, and identity fraud.

QUALIFICATION MISREPRESENTATION

Misrepresentation of qualifying circumstances is a methodology used to obtain payments that individuals are not entitled to receive. This includes providing false statements either online, in writing or over the phone, as well as providing false images to demonstrate the effects of a natural disaster.

FALSE STATEMENTS

To meet eligibility rules, false information provided in the process of claiming a disaster or emergency payment includes:

- falsely declaring employment status, income and hours of work lost due to an emergency or disaster
- exaggerating the extent of the damage from a natural disaster, whilst being geographically located in the impacted area
- updating a principal place of residence to be located within a declared disaster zone, despite the claimant not actually residing at this address during the declared period of the disaster
- providing dishonest statements regarding damage to possessions or property, such as claiming for damage whilst residing in a rented residence where the claimant is not financially responsible for the damaged asset.

FALSE IMAGES

As part of a natural disaster related claim, proof of the impact of the natural disaster is usually required. This includes photos of damaged property or possessions. It is increasingly common for those seeking to commit fraud to support applications with forged images or images obtained online.

ORGANISED CLUSTER FRAUD

Organised cluster fraud involves a central facilitator recruiting willing accomplices and coordinating their claims to optimise the chance of success. This fraud type can include:

- clusters of individuals who do not qualify for emergency or disaster payments lodging multiple claims with similar information to increase the likelihood of success
- a central facilitator who provides the benefit of experience likely from their own successful application and guides the claimants through the process
- a central facilitator who may prey on vulnerable people or groups to participate (e.g. non-English speaking, elderly, financially insecure, etc). Accomplices have varying levels of complicity.

There may be commonalities between the central facilitator and their accomplices such as attendance, participation or membership at a community or sporting group, a small town or even a residential address. The incentive to this organised approach can be in the form of payments back to the central facilitator.

In clustered frauds, successfully claimed benefits are generally paid to the legitimately and historically-accurate accounts of the claimants rather than fraudulently created accounts and profiles.

CASE STUDY:
ORGANISED CLUSTER FRAUD

After a March 2021 flood event in New South Wales, 51 individuals claiming to live in a specific location in the state, each made separate claims for the Australian Government Disaster Recovery Payment. The address reported by the claimants as being affected by the natural disaster was specific accommodation.

Individuals from this claimant cluster were all guests at the accommodation and were not financially responsible for damage to the building or furnishings.

As a result of Services Australia's investigations, debts were raised for each fraudulent claim totalling $42,500. All claimants received prosecution warning letters. The timely response in detecting this cluster and undertaking alternate interventions disrupted further fraudulent claims.

IDENTITY FRAUD

Identity fraud is a growing concern for all forms of financial government assistance. Reduced identity verification controls are sometimes necessary to deliver timely payments to emergency and disaster victims who may not have sufficient documentation to confirm their identity. This creates an increased risk for financial institutions and government to mitigate against identity fraud.

Identity fraud presents the greatest risk in emergency and disaster payment fraud due to the additional exploitation victims face following the compromise of their identity. This methodology involves a third party pretending to be the victim or victims in order to obtain emergency or disaster payments in the victim's name. This can include the use of a victim's identification or the creation of false identification information.

To receive the fraudulently obtained emergency or disaster payments, offenders may use their own bank account, a fraudulently created account in a victim's name, or a genuine account in the victim's name they have access to or some level of control over. Depending on the method used to receive payments, offenders may rapidly transfer the funds to another account, or move through numerous accounts before depositing into a useable account.

CASE STUDY: IDENTITY FRAUD

An individual (later identified to be 'the offender') collected detailed information relating to 19 different victims. With this information, the offender was able to use false identity information about the victims to create government profiles and update mobile phone and bank account details with Services Australia. The changes the offender made to the Government profiles facilitated the processing of Australian Government Disaster Recovery Payment claims and the receipt of payments to the offender.

In this fraud, the offender used two unauthorised bank accounts to receive 16 claims. Investigations identified that one of the accounts had been the offender's primary bank account (recorded with Services Australia since 2018). Furthermore, two of the offender's victims were family members, whilst address histories or matched identities found many victims resided in the same geographical areas. This is likely how the offender was able to gain the victims' personal information to take over their Services Australia profiles.

FRAUD INDICATORS

CASE STUDY: IDENTITY FRAUD

One offender claimed Australian Government Disaster Recovery Payments under 11 stolen/assumed identities and 54 false identities in addition to his own genuine identity. The offender received payments totalling $35,000 into three bank accounts. The offender also attempted to claim the JobSeeker payment, including the Coronavirus Supplement using three assumed identities. The offender continued to modify their way of operating to commit further offending. Following investigation and trial, the offender received a sentence of 4 years and 6 months imprisonment.

No single financial indicator will definitively identify if an emergency or disaster payment is fraudulent. Instead, financial institutions should use a combination of indicators in this report and business knowledge to conduct further monitoring and identify if a SMR needs to be submitted to AUSTRAC.

PAYMENT INDICATORS

The Reserve Bank of Australia deposits emergency and disaster payments into customer accounts on behalf of Services Australia. When these payments are deposited, they have specific payment descriptors, pay identity codes and have a set value amount. For example, COVID-19 Disaster Payments for Sydney during the first week of July 2021 contained the payment descriptor *'COVID-19 Disaster Payment (20 hours or more) – Sydney 1 to 7 July 2021'.*

GENERAL INDICATORS

BANKING PROFILE

- Known suspicious or blacklisted accounts receiving emergency or disaster payments.
- An account with limited or no genuine/everyday transactional activity receiving emergency or disaster payments.
- The same bank account receiving multiple emergency or disaster payments referencing different Centrelink Customer Reference Numbers (9 digits) or separate individual's names.
- Different bank accounts with the same account holder receiving emergency or disaster payments referencing different Centrelink Customer Reference Numbers or separate individual's names.
- Profiles with minimum, limited or no recent proof of identity documentation receiving emergency or disaster payments (they may also have been inactive for a period of time).
- A new to bank customer opening multiple accounts in a short period of time with no clear purpose can be indicative of intended future receipt of fraudulent disaster or emergency payments. Particularly where:
  - accounts are designed for online access and have no debit cards
  - accounts with debit cards but the card is either not requested, or it is issued but not activated
  - paper mail is sent to the recorded addresses and is returned.

FUND UTILISATION OR MOVEMENT

- Cash withdrawal of all received funds.
- Purchase of luxury goods such as designer clothes and bags.
- Holiday related expenses including accommodation and flights.
- Frequent use of payment applications to move funds between accounts.
- Emergency or disaster payments transferred to overseas accounts.
- Payment to digital currency dealers or platforms (often small amounts less than $100).
- Structured movement of money post emergency or disaster payments into suspicious accounts.
- Payments to gambling services (online or in person) or withdrawals in gambling venues.
- Shares, cryptocurrency or commodity trading related payments using the support payments.
- No or minimal payments made for repair work/maintenance or temporary accommodation.
- Movement of funds immediately post receipt of emergency or disaster payments into suspicious accounts.
- Numerous payments to hotels and/or accommodation providers (indicating offenders' are moving often or transient).

QUALIFICATION MISREPRESENTATION INDICATORS

- Payment descriptors for emergency or disaster payments indicate they are for a downturn in work; however, no decrease to regular salary is observed.
- Emergency or disaster payment references relate to an emergency or disaster that does not coincide with the customer's address (e.g. customer residing in Western Australia receives payments for the New South Wales floods).

ORGANISED CLUSTER FRAUD INDICATORS

- Rapid withdrawal of the value of emergency or disaster payments either in cash or to another account.
- Smaller transfers out from the claimant's accounts either shortly before or after the emergency payment is deposited. This may be a rounded percentage of the total emergency payments, or rounded whole amounts serving as fees to the facilitator.

IDENTITY FRAUD INDICATORS

- Newly created account with minimal activity receiving emergency and disaster payments.
- Recent updated contact information for accounts receiving emergency and disaster payments.
- Biographical inconsistency in accounts receiving emergency and disaster payments, such as names or descriptions of customer circumstances not corresponding to each other.

IDENTITY FRAUD VICTIMS

Victims subjected to a fraud attempt or identity compromise once, are more likely to have their details used for additional fraud attempts or scams. The victims are also more likely to be targets in future scams due to their vulnerability.

Stress (including financial) and loneliness increase an individual's chances of falling victim to a fraud or scam. Natural disasters and emergencies such as COVID-19 can also increase an individual's vulnerability. Offenders will take advantage of a person's circumstance and commence a cycle of victimisation against them.

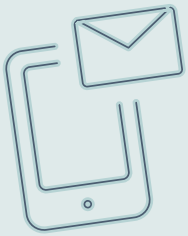
Prevention, by educating individuals on how to avoid falling victim to fraud attempts in the future is the best defence against initial and follow up fraud attempts. Where this fails, early detection also protects victims against emotional and financial loss.

REPORTING SUSPICIOUS BEHAVIOUR

One of these indicators may not suggest illegal activity on its own. If you see a combination of these indicators or observe other suspicious activity, consider submitting a SMR to AUSTRAC.

High-quality, accurate and timely SMRs give us the best chance to detect, deter and disrupt emergency and disaster support payment exploitation and other criminal activity.

To find out more visit: austrac.gov.au/smr



FOR MORE INFORMATION

If you have questions about your AUSTRAC compliance obligations, please email contact@austrac.gov.au or phone 1300 021 037.

More information about Services Australia's approach to serious fraud and identity crime is available on the Services Australia website.

NOTIFY SERVICES AUSTRALIA OF SUSPECTED FRAUD

If you suspect someone may be committing fraud against Services Australia, report it to Services Australia:

- fraud tip-off line on 131 524
- Reporting Fraud page
- Services Australia
  Reply Paid 7803
  Canberra BC ACT 2610

AUSTRAC.GOV.AU

1300 021 037

contact@austrac.gov.au