Australian Government
AUSTRAC

Fintel Alliance
An AUSTRAC initiative

Transfer and Pay
To:
Change
Amount
Description
This will appear on their statement and yours.
Reference
Paid By
This name will appear on their stat
Set as a sched

PREVENTING **MISUSE** AND **CRIMINAL COMMUNICATION** THROUGH PAYMENT TEXT FIELDS

FINANCIAL CRIME GUIDE NOVEMBER 2021

COPYRIGHT

ATTRIBUTION

ACKNOWLEDGMENTS

This financial crime guide was developed by AUSTRAC's private-public partnership the Fintel Alliance.

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 has been developed to raise awareness of the increasing misuse of financial transaction payment text fields being used to communicate between criminals or with victims for the purpose of harassment, intimidation or abuse.

Financial service providers should use the indicators in this guide to review their profiling and transaction monitoring. This will assist to target, detect and disrupt the use of the payment text fields in financial transactions by criminals and those seeking to gain access to, control and intimidate victims.

Financial service providers should use indicators in this report and their own business knowledge to conduct further monitoring and identify if a suspicious matter report (SMR) needs to be submitted to AUSTRAC.

⚠ This guide contains references to suicide, domestic violence and family violence that some readers may find distressing. Resources are included on page 13 if you or someone you know requires support.

ABOUT FINANCIAL CRIME GUIDES

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

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

If you identify indicators of criminal communication, abuse or other criminal activity through payment text fields and determine a SMR is necessary, the combination of well-articulated verbal and transactional indicators allows for better responses and actions by AUSTRAC and our law enforcement partners.

ABOUT THE FINTEL ALLIANCE

The Fintel Alliance is a public-private partnership led by AUSTRAC that brings together government, law enforcement, private and academic organisations 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 in Australia and overseas.

IMPORTANCE OF PARTNERSHIPS

Public-private partnerships are an effective way to identify, target and disrupt the misuse of payment reference fields in transactions to harass or abuse victims, or allow criminals to communicate undetected.

The Fintel Alliance members recognise the criminal misuse of payment text fields as a serious risk and uses its public-private partnership to target, disrupt and deter this offending to protect the community.

INTRODUCTION

Advancements in technology have increased the pace and complexity of financial transactions. As the volumes have increased so too has the amount of information that can be contained in each transaction enabled by new technologies and payment platforms. Individuals can make and receive payments in close to real-time, outside of normal business hours and there are now larger character limits within payment text fields.

The Fintel Alliance has identified an increase in the misuse of payment text fields in financial transactions as a method of criminal communication or abuse, rather than the primary purpose of transferring funds. Instead the transaction text fields are being used with increasing frequency to communicate for the purpose of stalking, harassing and threatening behaviour, or to avoid law enforcement scrutiny.

Communication within payment text fields is not unique to the Australian banking industry. Any payment that contains a free text field to be completed by the sender and viewed by the recipient can be a vehicle for criminal communication.

Individuals sending messages via this method may be unaware their activity will be scrutinised by their financial service provider, or are undeterred by the consequences of their actions.

Westpac research shows that one in two (51%) Australians have received some form of online abuse, including via email, mobile and social media channels. One in four (26%) admit to having used some form of inappropriate language in payment transactions.[1]

A recent survey conducted by YouGov and commissioned by the Commonwealth Bank of Australia showed that almost 40% of Australians say they have experienced or know someone who has experienced financial abuse.[2]

The New Payments Platform and overlay service Osko by BPAY allows for increased character limits (up to 280) and the use of emojis within payment text fields. The platform enables interbank payments to be sent in near real-time at any time of the day.

[1] https://www.westpac.com.au/about-westpac/media/media-releases/2021/9-february/

[2] https://www.commbank.com.au/articles/newsroom/2020/11/financial-abuse-hidden-epidemic-next-chapter.html

MISUSE OF PAYMENT TEXT FIELDS

Payment text fields are being used to communicate and facilitate serious offences by individuals and organised crime groups to coerce, threaten, stalk or harass their victim. The common themes identified within payments text fields include:

- technology-facilitated abuse
- threats or extortion attempts
- criminal communication
- threats of suicide and self-harm.

DEFINITIONS

Domestic violence refers to violent behaviour between current or former intimate partners – typically where one partner tries to exert power and control over the other, usually through fear. It can include physical, sexual, financial, social, verbal, spiritual and economic abuse.

Family violence is a broader term that refers to violence between family members, which can include violence between current or former intimate partners, as well as acts of violence between a parent and a child, between siblings, and more.[3]

Technology-facilitated abuse involves the use of technology including payment text fields as a communication method for an offender to coerce, threaten, stalk or harass their victim. Increasingly, this method is used by individuals who are the subject of protection orders, which constitutes a breach of the order.

Other crime types identified within payment text fields have included communications involving child abuse material, illicit drugs, firearms, ideologically-motivated extremism and outlaw motorcycle gang activity. Payments associated with these crime types include text relating to the purchase of a good or service rather than for communication purposes.

Where appropriate, AUSTRAC refers these matters to the relevant law enforcement agency for consideration of further investigation. In some instances, the criminal activity would not have been identified without financial service providers detecting and reporting the activity to AUSTRAC.

In instances where AUSTRAC or law enforcement involvement is not warranted, financial service providers are encouraged to undertake intervention actions to prevent further misuse of payment text fields. This can involve direct contact with the customer or their financial service provider, warning letters, suspension of financial services or in severe cases, termination of the customer's relationship with the financial service provider.

[3] https://www.missionaustralia.com.au/what-we-do/children-youth-families-and-communities/domestic-family-violence

IDENTIFYING THE MISUSE OF PAYMENT TEXT FIELDS

There is significant variance in the way individuals communicate via payment text fields. This coupled with the volume of payment messages sent, presents challenges for financial service providers attempting to identify and assess a payment text field's risk or severity. The different ways payment text fields can be used, and the challenges associated with identifying them are outlined below.

IS IT A THREAT OR A JOKE?

Payment text fields that make explicit threats to a victim or contain profanities that are considered abusive or offensive are commonly identified by financial service providers. However, a significant challenge in identifying legitimate instances of criminal communication is the high volume of false positives detected when cross referencing payment text fields with pre-established terms lists deemed to be inappropriate.

Words or phrases that have a dual meaning often appear in payment text fields and present detection challenges. The words 'pig' and 'dog' have an everyday meaning and appear in legitimate, non-threatening payment text fields but can also be used in a threatening or abusive manner.

CASE STUDY: EXPLICIT THREATS ARE NOT A JOKE

A financial service provider monitored and reported a series of suspicious transactions made to a 43 year old female that included threatening language within payment text fields.

A 33 year old male sent 170 payments including high volume, same day payments to the female over a five month period. The payments were valued at $1 or less and the payment text fields included references to reporting the offence to the police, labelling the recipient a pig and abusive and threatening language.

The offending was escalated to law enforcement for investigation with the offender apprehended for breaching a Protection Order.

CASE STUDY: REAL WORLD IMPLICATIONS

A 23 year old male was identified by a financial services provider after sending 10 payments valued at under $5 each with suspicious payment text to a female victim over five weeks.

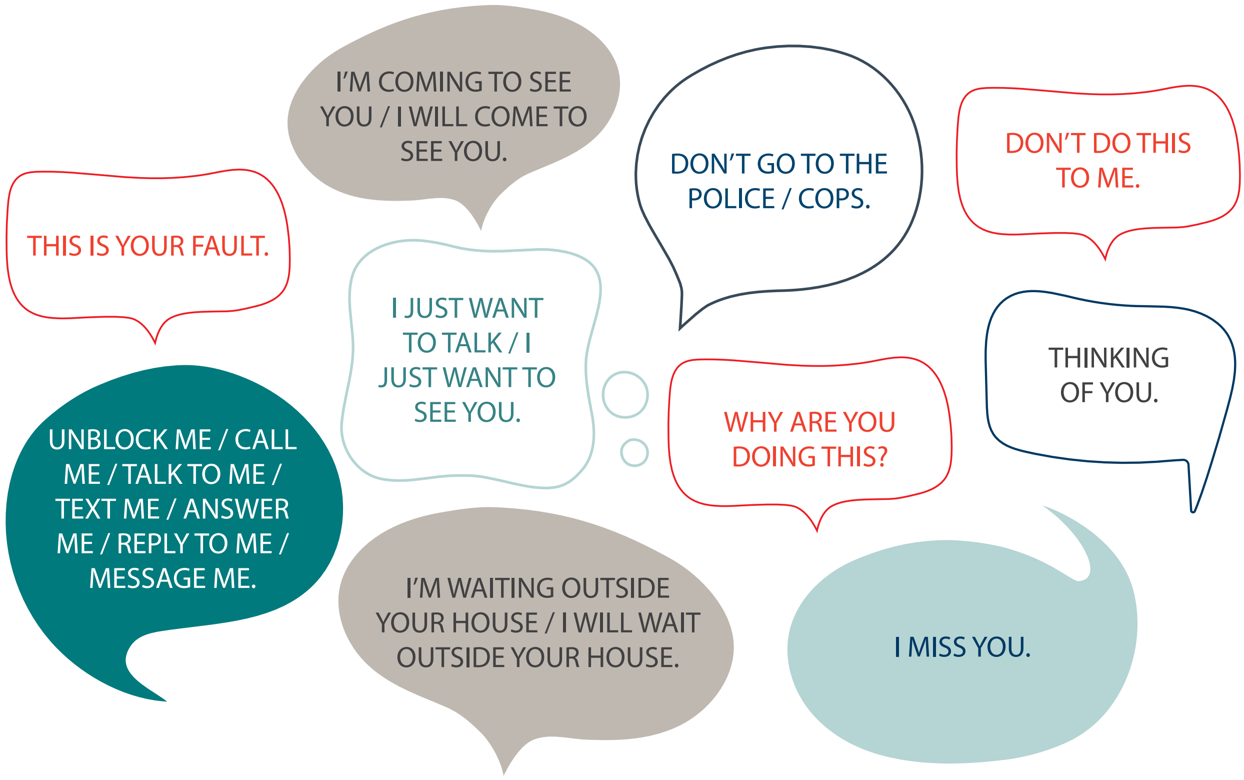
Messages within the payment text fields requested the victim contact him, as well as threats that he was planning to take his own life.

This matter was reported to AUSTRAC and following further analysis was referred to the State Police Force. The police investigation identified these messages had been sent in breach of a Protection Order taken out against the sender.

He was arrested and charged for breaching the Protection Order by communicating with the victim via financial transactions.

INCONSPICUOUS PAYMENT MESSAGES

A lack of offensive or abusive language does not deem a payment message harmless. Some perpetrators of technology-facilitated abuse remove explicit threats or profanities in an attempt to legitimise payment text or avoid scrutiny by financial service providers. Some payment text do not contain overtly threatening language but when accompanied by high volume or low value payments may be harmful. These payments may not be identified through key word analysis of payment text fields.


THIS IS YOUR FAULT.
I'M COMING TO SEE YOU / I WILL COME TO SEE YOU.
I JUST WANT TO TALK / I JUST WANT TO SEE YOU.
DON'T GO TO THE POLICE / COPS.
DON'T DO THIS TO ME.
THINKING OF YOU.
UNBLOCK ME / CALL ME / TALK TO ME / TEXT ME / ANSWER ME / REPLY TO ME / MESSAGE ME.
WHY ARE YOU DOING THIS?
I'M WAITING OUTSIDE YOUR HOUSE / I WILL WAIT OUTSIDE YOUR HOUSE.
I MISS YOU.

THE USE OF ABBREVIATIONS AND SLANG TERMINOLOGY TO HIDE MEANING

Due to character limits, payment text fields often contain abbreviated, shortened and/or slang words. A sender that is conscious of transaction monitoring may also attempt to hide their messages by substituting letters for symbols (e.g. the letter 'S' for $) or breaking up words with spacing (e.g. 'die' to 'd i e'). This means the payment text of concern may not be easily identified if transaction monitoring models do not account for incorrect spelling and abbreviations used in payment text fields.

REFERENCES TO SELF-HARM AND SUICIDE

Threats of suicide and self-harm are also evident within payment text fields. These payments have been seen with and without explicit or abusive language and do not always contain words such as 'suicide' which can present challenges detecting them. References to self-harm or suicide may be seen after a series of earlier messages demonstrating a pattern of escalating behaviour.

Any mention of suicide or self-harm is serious and presents welfare concerns for the individual contemplating these actions, but also for the recipient of such messages who may find them distressing. Conversely, messages containing threats of suicide or self-harm can be used as a form of power and control. For example "I love you so much and I can't live without you, if you leave me I'll kill myself." These words can be used by the perpetrator to convince someone who is experiencing domestic or family violence to feel overwhelmed by guilt and confusion, and ultimately, stay in an abusive and potentially lethal relationship.

EMOJIS

Some payment platforms have the capability for emojis to be included in payment text fields. Different emojis can be used to convey threatening or abusive messaging to a payment recipient. This can include emojis depicting weapons, injury or death, or a sexual connotation.

CRIMINAL COMMUNICATION

Criminals may use the payment text fields in transactions to avoid law enforcement scrutiny of their criminal activities. This can include small value payments referencing the supply or shipment of illicit goods or a planned event. This type of offending will take the form of a two way conversation with small value payments sent between individuals.

FINANCIAL INDICATORS

Financial indicators can assist financial service providers to conduct further monitoring and identify if a SMR needs to be submitted to AUSTRAC.

VALUE

- Payments can be as low as $0.01 and are typically below $10.
- Higher value payments often represent an exchange for goods or services.
- Payment values may suddenly increase as a result of a warning by a financial service provider to avoid further scrutiny.

VOLUME

- High frequency payments are conducted in a short period of time, and may include more than one low value payment made in the same day or month.
- Exploitation of payment text fields is more likely to occur when a high frequency of payments are sent over a prolonged period.

RELATIONSHIP

- Analysis of all payment text fields exchanged between two parties within a fixed period can assist to determine any patterns and provide context if the matter is indicative of offending.
    - One person sending low value payments with no reciprocal reply is more likely indicative of abuse or harassment.

PAYMENT TEXT FIELDS

- Seemingly non-threatening or non-emotive language can still be considered threatening or concerning.
- Blank payment text fields, or those only including the customer or sender name combined with high volume and/or low value payments can be indicative of threats or harassment.
- Incorrect spelling is used to fit messages within character limits, to avoid obvious detection by financial service providers and is also seen in slang terminology.

STOPPING ABUSE IN ITS TRACKS

To protect customers from abusive messages via payment text fields some financial service providers have implemented new measures to identify abusive or offensive inbound payment text and block inappropriate outbound payment text. To enable comprehensive assessment of incoming and outgoing payment text fields, financial service providers are employing multiple techniques to maximise scrutiny.

TERMS LISTS AND LEXICONS

Terms lists of words known to be offensive or threatening assist with identifying payments of concern. Terms lists can be used with other measures to analyse large numbers of transactions to identify instances of abuse or criminal communication.

A lexicon is a compilation of keywords or terms related to specific themes (e.g. profanities, threats, illicit drugs, etc.). Payment text fields sent and received by customers can be reviewed against these compilations and if a match or matches are detected, the payment text can be escalated for further review.

Manual scrutiny of payment text that match keywords or terms within lexicons can be time intensive, yield a high false positive rate and lead to challenges identifying slang, misspelling, coded messaging and less obvious threats.

SENTIMENT ANALYSIS

Sentiment analysis is a method for determining the sentiment (e.g. positive, negative or neutral) of a word or phrase. Sentiment analysis relies on an established lexicon or a sentiment library containing terms that have been pre-determined as negative, positive or neutral to assess the overall sentiment of a word or phrase.

In a financial setting words generally considered negative may not be useful in identifying criminal communication through payment text fields. For example, the words 'tax', 'fee' and 'late' are commonly associated with legitimate financial payments. However, seemingly neutral words such as 'call', 'block', 'blocking' and 'unblock' are used by offenders of technology-facilitated abuse when requesting a victim to call them back, answer their calls, unblock them or ask why they were blocked on social media or phone.

INBOUND PAYMENTS

Some financial service providers have introduced the ability for customers to report or flag offensive payment text which is then referred for assessment. As part of this assessment, further action is considered against the reported abuse such as providing a warning to the customer or reporting the matter to the sender's financial institution or reporting a SMR to AUSTRAC. Reported text is also used by financial service providers to detect future abusive content.

OUTBOUND PAYMENTS

Financial service providers have implemented technology to monitor outgoing payments sent through different platforms. This technology is used in real-time to block transactions deemed to contain inappropriate or offensive language. Customers whose outgoing payments are blocked are notified that their transaction contains inappropriate language. For the payment to be accepted and sent, the customer is required to remove the inappropriate language from the transaction.

Continued technological advancements to payment platforms will present future challenges, with offenders able to modify their behaviour to enable offending. As those exploiting payment text adapt, it is important that financial service providers understand and respond to emerging techniques used to facilitate this offending behaviour.

Financial service providers have demonstrated innovation in responding to this emerging risk to the community. The use of real-time monitoring, customer self-reporting and in-depth data analysis has reduced the risk of criminal misuse of payment text fields.

REPORT SUSPICIOUS MATTERS TO AUSTRAC

Financial service providers should use the indicators in this report combined with their own business knowledge to conduct further monitoring and identify if a suspicious matter report (SMR) needs to be submitted to AUSTRAC.

High-quality, accurate and timely SMRs give us the best chance to detect, deter and disrupt abuse, criminal communication and other criminal activity via payment text fields to help protect Australians.

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.

Domestic and family violence support is available by calling 1800 737 732.

1800RESPECT

1800RESPECT is a 24-hour national sexual assault, family and domestic violence counselling line for any Australian who has experienced, or is at risk of, family and domestic violence and/or sexual assault.

Phone: 1800 737 732

Website: https://www.1800respect.org.au/

MEN'S REFERRAL SERVICE

The Men's Referral Service is a free, confidential telephone helpline that offers counselling, advice and support to men who have anger, relationship or parenting issues.

Phone: 1300 766 491

Website: https://www.ntv.org.au/get-help/

For immediate support call Lifeline on 13 11 14 or Beyond Blue on 1300 224 636.

LIFELINE

Lifeline is a national charity providing all Australians experiencing emotional distress with access to 24 hour crisis support and suicide prevention services.

Phone: 13 11 14

Website: https://www.lifeline.org.au/

BEYOND BLUE

Beyond Blue provides information and support to help everyone in Australia achieve their best possible mental health.

Phone: 1300 224 636

Website: https://www.beyondblue.org.au/

In an emergency, call the police on 000.

FOR MORE INFORMATION ABOUT DOMESTIC AND FAMILY VIOLENCE

White Ribbon Australia: Prevent Men's Violence Against Women

Website: https://www.whiteribbon.org.au/

AUSTRAC.GOV.AU

1300 021 037

contact@austrac.gov.au