Australian Competition & Consumer Commission

A guide for business

Best practice guidelines for dating sites:

protecting consumers from dating scams

January 2016

Online dating sites offer services to facilitate relationships between their members and this has become a popular form of social networking. However, the online environment also provides opportunities for scammers, including international criminal networks, to target Australian consumers.

ISBN 978 1 922145 72 7

Australian Competition and Consumer Commission
23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601

ACCC 01/16_1062

www.accc.gov.au

Foreword

I am pleased to present this revised edition of the *Best Practice Guidelines for Dating Sites*. These guidelines aim to help online dating site operators respond to scams targeting their users.

Online dating scams are often the work of international criminal networks and cause significant harm to Australian consumers. In 2015, the Australian Competition and Consumer Commission (ACCC) received over 2600 reports of online dating scams and consumers reported nearly $23 million in losses to these scams. In 2014, over $28 million in losses were reported. These amounts are likely to be much larger because many others will have not reported losses or reported elsewhere. In addition to losing money, many victims of these scams also report serious emotional harm. Similar scams are targeting Australian consumers through social networking sites and the ACCC is also looking at what can be done to prevent scammers using these channels.

The guidelines have been developed by a working group, chaired by the ACCC and comprising of representatives from a number of dating sites. Many dating sites have already implemented substantial measures to protect their users from scams. The challenge is to build upon these measures and bring consumer protection across the whole of the industry to a high standard.

For those sites that already have measures in place to protect against scammers, the objectives of the revised guidelines are to:

- strengthen the targeting, relevance and timeliness of warning measures
- ensure effective complaint handling, and
- promote vigilance to prevent scammers operating on their sites.

For those sites that are new to the industry or don't yet have such measures in place, we strongly encourage you to use the guidelines provided to protect your users from such scams.

While the guidelines are not mandatory, the ACCC considers that they represent industry best practice and encourages their adoption and implementation by all dating sites that are used by Australian consumers. Consumer confidence and trust is vital to the online dating business model and is undermined when consumers fall victim to scammers.

These guidelines have been designed to be flexible and adaptable to meet the needs and resources of different dating sites and can be tailored to suit the characteristics of their users.

The ACCC recognises and appreciates the contribution of participants in the online dating industry to the development of the guidelines and their willingness to ensure the guidelines reflect the needs and concerns of both the industry and its users.

Delia Rickard

Deputy Chair
Australian Competition and Consumer Commission

Contents

Best practice guidelines for dating sites—protecting consumers from dating scams

Context

Introduction

1. Online dating sites offer services to facilitate relationships between their members and this has become a popular form of social networking. However, the online environment also provides opportunities for scammers, including international criminal networks, to target Australian consumers.

2. Reported losses by Australian consumers to online dating scams are very high. Typically, the scammer will create fake profiles and contact legitimate users for the purposes of financial fraud and identity theft. They will form a relationship with a legitimate user, sometimes over a significant period of time, and then defraud them. Scammers may also launch concerted attacks to commit identity theft.

3. Victims of these scams often suffer significant financial losses, as well as emotional harm. Scam activity can also have a detrimental effect on the online dating business model by undermining consumer confidence in the service.

4. It is in the interests of all online dating site operators to take action to disrupt the activities of scammers targeting their customers by offering a safe and secure operating environment and providing advice to consumers on measures they can take to protect themselves.

5. Educating consumers about using online dating sites safely is important to both online dating sites and law enforcement alike. Both have the shared objective of disrupting and preventing illegal activity.

6. The development of the best practice guidelines (the guidelines) by the Australian Competition and Consumer Commission (ACCC) and the online dating industry has drawn upon measures that many online dating sites have already implemented. The development and revision of the guidelines has been undertaken to counter the activities of scammers and provide guidance to the industry on how to better inform and protect their users.

7. The actions detailed in the guidelines are divided into four categories:

   7.1 Appropriate scam warnings and information—

   - Appropriate scam warnings and information are necessary to educate consumers and raise awareness of the risk of scams.
   - Scam warnings should include simple and direct key messages, as well as examples. A set of example key messages for use by online dating sites is attached to these guidelines.
   - Consistent messaging across online dating sites may enhance the effectiveness of these warnings. Online dating sites can make use of the attached warnings and adapt the wording to suit their individual needs, while retaining the essential message.

   7.2 Vetting and checking system—

   - A robust vetting and checking system to identify scammers both as they attempt to register with a site and following registration is an important tool for online dating sites to disrupt the activities of scammers.

   7.3 Complaint handling procedures—

   - Effective complaint handling procedures are vital for online dating sites to respond to scams. They allow for scammers to be quickly identified and action taken to protect users, including warning others a scammer has communicated with. Such procedures must be easily accessible to users, responsive to their complaints, and informative.

7.4 Consumer Protection—

- Compliance with the *Competition and Consumer Act 2010* ensures consumers are provided with upfront and transparent information upon which they may make informed decisions and that they are not subjected to unfair contract terms. This section is provided to assist online dating sites to understand their obligations under Australian consumer law in the context of industry specific issues that have previously arisen.

Scope

8. The guidelines are suitable for adoption by all online dating sites, including those operating as an application (app) on a mobile device. The guidelines are relevant to all dating sites used by Australian consumers, whether they are based in Australia or overseas.

Objective

9. The guidelines seek to protect Australian consumers by providing a set of actions for implementation by online dating site operators to improve their response to scams.

10. The guidelines are voluntary and are intended to represent best practice.

11. All online dating site operators should consider implementing the actions contained in the guideline, supplemented by any additional actions they identify as effective.

12. The actions detailed in the guidelines are intended to be flexible and their implementation should be adapted to fit the layout, user base and business model of each individual online dating site.

13. The attachments to the guidelines provide material which may be used by online dating site operators for warning messages and to inform their users about scams.

14. Adoption of the guidelines is not a replacement for overall compliance with the *Competition and Consumer Act 2010* or other legislation. The ACCC does not endorse sites or vet their compliance with the guidelines. Businesses should obtain their own legal advice as to their obligations under consumer protection legislation.

The guidelines

Appropriate scam warnings and information

15. In order to educate and inform their users, online dating sites should provide information and warning messages about scams. Warning messages should include both key messages and examples in appropriate locations.

Display of warning messages

16. Warning messages should be clearly and prominently displayed at appropriate locations on the online dating site in a form likely to be noticed and make an impact on users, such as a banner, sidebar, insert or link to further information.

17. The appropriate location for warning messages may vary, depending on the layout of the site but should be where the messages will be regularly viewed by users, particularly at 'points of decision' where users may be contacted by scammers.

18. For example, warning messages may be displayed:
    - where members communicate including chat, instant messaging, email and other communication services provided by the site
    - at any other relevant locations frequently visited by site users.

19. Using data to identify at risk groups, online dating sites can actively provide tailored warning information to users that are more vulnerable, e.g. analysis of demographic data has consistently shown 45–65 year olds are commonly targeted by these scams. Providing warnings to at risk groups could be achieved by sending an email on completion of the sign-up process or by redirecting at risk users to tailored messaging on an additional internet page as part of the registration process.

20. It is well known that scammers encourage their targets to move away from secure communication channels to other methods of communication where the risk of detection is lower. Online dating sites can provide an initial warning of this and warn users again when they are closing their accounts with the site.

Content of warning messages

21. As part of their warning messages, online dating sites can display key messages to warn their users about the risk of scams.
    - To be most effective, key messages should be simple and direct.
    - Key messages should be appropriate to the area of the site on which they appear.

22. A set of example key messages for use by online dating sites is at attachment A. Use of these example messages will reinforce the consistency of warnings across the industry. However, sites can also adapt the exact wording and location of these messages to suit their layout and the needs of their user base.

23. Online dating sites may also develop additional key messages which they consider effective. These messages should also be simple, direct and consistent with those in attachment A.

24. In addition to key messages, online dating sites should consider displaying warning messages consisting of examples of scammer conduct. Users are more likely to be responsive to warnings in the form of a real situation or story they can recognise.
    - Examples may be displayed in a brief format in the same locations as key messages, or with more detail elsewhere on the site.
    - Steps should be taken to draw the attention of users to these more detailed examples, such as through a link contained in a warning message.

25. A set of examples of scammer conduct is at attachment B. However, sites can also adapt the exact wording of these examples to suit their layout and the needs of their user base.

26. Online dating sites are encouraged to develop additional examples based on their own experience of scams.

27. Online dating sites should also regularly review their examples to ensure they reflect current trends in scammer behaviour and to warn users about new and emerging scams.

28. It is not expected that all key messages and examples will be displayed together at one time. Instead, key messages and examples should be appropriate to the location where they are displayed and may be part of a changing set of such messages.

Provision of detailed information

29. Online dating sites should provide their users with access to detailed information on scams. This information may be provided as part of the site, or on a separate dedicated online safety page.

30. The attention of users needs to be drawn to this information. For example, the information or a link to the information could be provided:
    - as part of information on how to use the sites provided to new members at the end of the registration process or soon afterwards—for example, in a 'welcome' email or internal message sent to new members
    - during regular communications with members—such as a newsletter or update service
    - through links within the online dating site where appropriate.

31. Online dating sites may also display a link to scam information on their homepage.

32. The detailed information should be sufficient to fully inform users about the risk of scams and how to identify and protect themselves from scams.

33. This information may include:
    - warning signs when a user is communicating with a scammer
    - common stories used by scammers when they request money
    - steps to be taken if a user thinks they have fallen victim to a scam (see paragraph 52)
    - any other information relevant to educating users about scams.

34. The detailed information may be presented in the form of a Frequently Asked Questions (FAQ) page. An example FAQ is at attachment C.

35. Online dating sites may provide a link to the ACCC's scamwatch website (www.scamwatch.gov.au), which contains information about a variety of scams, including online dating scams, but site operators should also maintain information about online dating scams on their own site.

36. Detailed information should be regularly reviewed for accuracy and updated to reflect current trends in scammer behaviour.

Social media, mobile sites and smartphone applications

37. Many dating services have developed applications ('apps') designed specifically for use with a smartphone or other device. Some dating services may only operate through an app. These guidelines are suitable for adoption by all dating sites, including those operating as an app on a mobile device.

38. Many dating sites will also operate social media accounts. Responsible dating sites will display simplified scam warnings and/or prominent links to information about scams on all communication channels, having regard to and in keeping with the objectives of the guidelines.

Vetting and checking system

39. Responsible online dating sites validate users to ensure legitimate use of the service and minimise the ease with which scammers can create fake profiles. Online dating sites should consider implementing validation procedures, including the collection of sufficient information to authenticate the identity of an individual during the registration process.

40. While it may not be possible to identify all scammers, online dating sites can implement a robust vetting and checking system intended to identify scammers as they attempt to register with the site and following registration.

41. A robust vetting and checking system would consider a range of different characteristics of user profiles, user behaviour and other data in order to identify those profiles which have been created by scammers and remove them from the site.

42. For example, characteristics which may be checked by such a system include:
    - the language used in the profile, including identification of common phrases used by scammers, common usernames and passwords used by scammers and a prevalence of spelling/ grammatical errors
    - checking of profile pictures, to identify common pictures used by scammers
    - checking of Internet Protocol (IP) addresses to identify users registering from outside Australia (where appropriate) or from areas of the world linked to scam activity
    - measures to address the use of proxy servers and other methods to evade IP checking
    - abnormal behaviour by users within the site, such as the volume of messages sent or responded to
    - any other characteristics which are an effective way to identify profiles likely to be created by scammers.

43. Online dating sites can adopt a vetting and checking system that best fits their site structure and level of traffic. Such a system can involve manual or automated checks, or a combination of both.

44. Online dating sites may choose to outsource the vetting and checking of profiles by engaging the services of a commercial online security specialist.

45. As the methods used by scammers may change over time, online dating sites should regularly review their vetting and checking systems to ensure they remain effective.

Privacy

46. Online dating sites have obligations to protect all customers' personal information and comply with privacy laws. The purpose of many known scams is to facilitate identity theft which, in turn, enables further scam conduct. Online dating sites should have in place security systems to guard against the loss of any consumer's personal details.

47. In the event of a security breach, online dating sites should have in place processes to alert customers and former customers (if affected) that such an incursion has occurred. This should include advice to affected parties about the nature of the information that has been compromised and steps they may take to guard against future misuse of that information, e.g. if credit card information is compromised, affected parties should be advised to immediately contact their financial service provider.

48. The Office of the Australian Information Commissioner has developed guidance on *Data breach notification— A guide to handling personal information security breaches* which focuses on the steps an agency or organisation can take after a data breach involving personal information occurs. Online dating sites are encouraged to adopt these guidelines and proactively put in place a data breach response plan.

Complaint handling procedures

49. In order to identify scams, gather information and assist affected users, online dating sites should provide complaint handling procedures where users can report a scam and ensure users are aware of this system.

Lodging a complaint

50. Responsible online dating sites have established mechanisms for users to report suspicious conduct within the online dating site—such as a button entitled 'report a scam', 'report abuse' or other words to similar effect. To maximise the effectiveness of this mechanism it should be available without the need for current membership to the service.

51. Operators may also provide a 'live help' feature to respond directly to affected users via chat, instant messaging, Voice over Internet Protocol (VoIP) or other methods.

Referring complaints

52. Online dating sites should implement the following referral process for Australian users who have identified or been affected by a scam:
    - advise users to report the scammer to the site operator first
    - advise users they can report the scam to the ACCC scamwatch site—www.scamwatch.gov.au
    - advise users who have sent money and provided financial details to contact their financial institutions and inform the provider of any service (such as a money transfer service) which they used to send money to the scammer. While it is rare that money can be recovered, advising banks and money remitters assists them to take action to prevent further fraud and potentially stop other victims from sending money to scammers
    - advise users who have lost money to a scammer, or where the scammer has threatened or attempted to blackmail them, to report the matter to the police via the Australian Cybercrime Online Reporting Network (ACORN) at www.acorn.gov.au

53. A template advice to users on what to do if they have fallen victim of a scam is at attachment D.

54. Non-Australian users who report a scam should be referred to their local consumer protection and legal authorities as appropriate.

55. As legitimate users may lose access to the site if their profile is hacked or mistakenly removed, online dating site operators should ensure that their customer service staff can be contacted via an alternative means or channel that does not require the user to be logged in.

Responding to complaints

56. Where the user seeks a response, online dating site operators should endeavour to respond to complaints of scam activity as soon as practicable, ideally by the end of the next business day. This response should include information on what action the user can take if they have fallen victim to a scam.

57. Upon receipt of a complaint about scam activity, responsible online dating site operators will investigate the profile alleged to be engaging in scam activity and take appropriate action as soon as possible.

58. Where a profile has been identified as being operated by a scammer, the site operator should notify other past and current users contacted by that scammer.

59. Staff dealing with customer complaints should receive training on the issue of scams.

60. Online dating sites should keep the details of customer complaints confidential and advise their customers that they will do so.

61. In order to monitor the effectiveness of their anti-scam measures and update them when necessary, online dating site operators should collect data on complaints about scams.
    - This data would include the number of complaints, the amount of money reported lost and the type of scam. The more data collected, the more useful it will be for improving security systems to aid scam prevention.

- The data is to be collected from the information provided by the complainant. It does not require online dating sites to seek further information from complainants, although you are encouraged to do so if it may help prevent scams.

Consumer protection

62. All businesses, including online dating sites, have obligations under the *Competition and Consumer Act 2010*. Fundamental to many of these obligations are provisions ensuring consumers are provided with upfront and transparent information upon which they may make informed decisions and are not subjected to unfair contract terms. This section is provided to assist industry to understand its obligations in the context of industry specific issues that have previously arisen.

63. Adoption of the guidelines is not a replacement for overall compliance with the *Competition and Consumer Act 2010* or other legislation. Businesses should obtain their own legal advice as to their obligations under consumer protection legislation.

Fees and charges

64. Online dating sites should clearly disclose all prices for dating services including any applicable fees and charges prior to the acceptance of any contract or request for payment.

65. Where online dating sites offer services on a subscription basis, providers should make it clear and disclose upfront that membership is a subscription that is automatically renewed and incurs ongoing fees until cancelled.

66. Online dating sites should clearly disclose the process for cancellation and accept notice of termination by email or other form of electronic communication (e.g. web form). D & R sites should ensure that cancellation processes are accessible and not onerous.

Use of personal information

67. Online dating sites should not use customer information for unauthorised purposes without express consent. Given the sensitive nature of the information provided, it should not be inferred from a customer's acceptance of general terms and conditions that they have consented to a broader use of their personal information, e.g. online dating sites shouldn't include a customer's profile on other sites without specific consent for each site—consent should be on an opt in basis.

Attachment A—Key messages

- Know who you're dealing with—never send money to anyone you have only met online.
- Contact from a person overseas makes it more likely that they are a scammer, even if they say they are just travelling for work.
- If someone asks you to transfer money to them via a wire service, don't do it—scammers also use money orders, bank transfers, pre-loaded cards and electronic currencies (e.g. bitcoin).
- Have you met someone recently and they've already professed their love? Be careful—it could be a scam.
- If someone you met online says they need your help or your money, it's probably a scam.
- If someone asks you for money, don't reply no matter what their reason is.
- Don't share your banking or credit card details with anyone you have only met online.
- Some scammers may ask for a loan or to co-invest in a business venture; typically with a too-good-to-be-true return on investment. Any 'investment' in these scams will equate to a loss.
- If you are asked to cash or deposit a cheque for someone you have only met online, don't do it. Scammers will ask you to send them money before the cheque clears and the cheques are always bad. NEVER commit to any bank or monetary transaction for someone you have only met online.
- If someone asks to move your communications outside the site after only a few contacts, be careful—scammers often ask for this.
- Anyone can fall for a scam—be careful and report any suspicious conduct here.
- Met someone who sounds too good to be true? Be careful—it could be a scam.
- If what you are seeing and hearing from someone does not match their profile, be careful— it could be a scam.
- Do an image search of your admirer to help determine if they really are who they say they are. You can use image search services such as Google or TinEye.
- Google search some of the phrases in emails they have sent you. You may find these have been used over and over again by scammers.
- Beware of accepting gifts that could be used to conceal drugs. Some scam victims have been caught carrying drugs through customs in luggage they were given as a present.
- Do not agree to transfer money or send valuable items for someone else: money laundering and drug trafficking are criminal offences.
- Never share intimate photos or videos with prospective partners, especially if you've never met them. Scammers are known to blackmail their targets using compromising material.

Attachment B—Examples of scammer conduct

The ACCC considers that the following could be used by online dating site operators as examples of scammer conduct, supplemented by their own experiences.

Short examples of scammer conduct

'Did you know that scammers will often tell you they need money for medical treatment, be it for themselves, a sick relative or child?'

'Scammers sometimes take a long time to build a relationship with you—never send money to anyone you meet online, no matter how long you have been chatting with them.'

'A common tactic for scammers is to ask for money for flights, visas or other expenses and promise that they will come and visit you—don't be fooled.'

'Some scammers will tell you that they are in the military and need money for a leave pass so they can visit you. This is a scam because you don't pay for leave passes.'

'Sometimes a scammer's description will not match their profile picture—be cautious and look carefully.'

'It is not a coincidence that the scammer's computer camera or Skype connection never seem to work.'

'Scammers may claim to be recently widowed to gain your trust, sympathy and money!'

Sometimes scammers ask for a small amount of money and will pay it back. They may also send small gifts. These are just tactics to gain your trust.'

'If anyone asks you for personal details such as banking details or credit card numbers, don't send them.'

More detailed examples of scammer conduct

'You should exercise caution wherever someone you meet online claims that they are stationed overseas as an oil worker, aid worker, as part of a peacekeeping force or other job. Scammers will often use this excuse and ask you to send money because of some crisis, like being robbed or becoming sick.'

'Needing money for a plane ticket or travel expenses to visit you is a common story used by scammers. They might ask you for money for a ticket, visa or immigration fees. They may instead send you a 'genuine' copy of their visa or plane ticket but then tell you they need money for an unexpected expense. Don't be fooled—scammers often have access to high quality fake documents.'

'Scammers don't just ask you for money. They may also ask you to provide personal details, such as your name and address, bank account or credit card numbers and use this information to steal your identity.'

'Scammers might ask you to transfer money for them through your account, telling you it is because they are unable to transfer the money themselves. You should never give out personal financial information to anyone you meet online because of the risk of identity theft. Transferring money may also involve you in money laundering, a serious crime, and expose you to criminal prosecution.'

'If you are asked to cash money orders for someone you meet online, you should not do it. Scammers often promise to send their victim money orders and ask the victim to cash the orders and wire the money back. However, the money orders are fake, so after sending money to the scammer, the victim finds themselves pursued by the bank for the value.'

'Been offered a big payout by someone you met online? Scammers will use all kinds of stories to get you to send money to them. They might tell you that the money will go to a charity, or be invested in a business like oil exploration or gold mining. Alternatively, they may promise that paying money will allow you to access a lottery prize, a long lost inheritance or treasure, like a cache of gemstones. What are the chances that you will find both true love and millions of dollars online? Don't respond to these offers.'

'A popular story for scammers is to claim to be a soldier, stationed overseas and to say they need you to send money for their expenses—often so they can purchase a leave pass to visit you. Don't be fooled—you should never send money to anyone you meet online.'

'When a scammer asks you to send money, they will usually come up with a whole series of excuses for why they need more. For example, a scammer who asks you for money for plane tickets may then tell you they need more money for customs fees and an exit visa and then tell you they have been arrested at the airport and need even more money to recover their possessions. You should never send money to anyone you meet online.'

'Be careful of sharing your personal information, such as your full name, address, birth date, family details or intimate photographs and videos with people you meet online. These may be used by scammers for the purposes of identity theft or blackmail.'

'Scammers may also ask you to send pictures or videos of yourself, possibly of an intimate nature. They may use these later to try and blackmail you by threatening to send them to your friends, family or employer.'

Detailed example of scam progression

Jessica, an Australian businesswoman in her 40s, met a man called Martin on an online dating site.

Martin's profile said that he was an Australian but he was currently working for an oil company in the United Arab Emirates. He said he was posted to the UAE for a brief period to oversee an oil pipeline project but was due to return home soon. He was a widower with a 10-year-old daughter. Martin's photo showed that he was attractive, well-dressed but not too formal. He looked friendly and about the same age.

Martin's interests were not very specific but appeared similar to Jessica's own, namely sports and other outdoors activities. Both were after a serious relationship and looking for a warm and loving partner.

Martin told Jessica that he could not reliably access the dating site in the UAE and so they moved their communications to email and phone.

Jessica and Martin struck up a close relationship and exchanged regular emails and many phone calls. Martin came across as sensitive and caring and often listened to her problems. He showed an interest in her life, including her business affairs. He liked to call just to tell her he missed her and would love to meet up. After several months Jessica felt that she could tell Martin anything and Martin confessed his love for her.

Soon afterwards, Jessica received an email from Martin claiming that he had been mugged and lost his wallet. He said that he was working away from his camp, and at the hotel where he was staying, the hotel manager was holding his passport and refused to return it until he paid his next month's bill. He was soon to be paid but asked Jessica to advance him $1200 by wire transfer to help with his hotel bill. Jessica thought he would pay her back so she wired the money across.

Some weeks later, Martin called Jessica in quite a state and told her that his daughter had been struck by a car in a hit and run on her way to school and suffered a brain haemorrhage. He said that he needed $8000 quickly, to pay for an expensive operation to save her life. Horrified by these events, Jessica sent the money via wire transfer as it would be quicker.

Things were settled for a while and then Martin told Jessica that he had an opportunity to invest in oil exploration in Ghana. The enterprise was to help out the poor local community and investors would be well rewarded. He said that she was guaranteed a big return if she sent him $40 000 to invest. He said that this would help them set up a home together when he returned to Australia soon. He also advised her to transfer the money from her bank to the investment account held at Barclays bank because this would be safer and he gave her all the relevant details.

Jessica was concerned because this was a large sum of money and asked her friends and relatives what she should do. Some of her friends expressed concern that she may be dealing with an online scammer.

Jessica questioned Martin's motives. He told her he was very hurt and sent her photographs which he claimed were photos of himself with his daughter and children in the local community. Jessica told her friends that she knew and trusted him and decided to send the money anyway.

Over time, Jessica was asked to help out in a number of ways as well as pay for fees and taxes on her 'investments' until she had paid over $90 000. Some of Jessica's friends showed her material about online scams, so Jessica began to keep details about the relationship to herself. However, when Jessica again mentioned her concerns to Martin, he told her that he "swore by almighty God" that he loved her and the money she sent was being invested in their relationship.

It was hard, but soon Jessica had to admit to herself that there was something wrong. She thought about how the conversations often turned to money and the requests for more were becoming very frequent. One day after he had asked for more money to organise travel to Australia she decided to stop. Martin's emails and phone calls became increasingly insistent and angry. She should have hung up straight away but she still felt something for him.

Then Jessica received an email threatening to send her friends and family copies of intimate photos Jessica had sent to Martin, unless she paid another $10 000. This cemented in Jessica's mind that the whole affair was an elaborate scam and Jessica finally sought help from the police.

Jessica felt devastated that a man she felt she could trust implicitly was in fact a scammer. In addition to these mental and emotional costs, she had also sent the scammer in excess of $90 000—most of her life savings.

She found it hard to discuss this with her family and friends because she felt so foolish. They had warned her but she trusted the scammer over those truly closest to her. When she did her own research she found that she was not alone. Many others had had similar experiences.

Attachment C—Example FAQs

What is a dating scam?

On a dating site, a scammer is someone who builds a relationship with you, pretending to be a legitimate user of a dating site, and then uses fraudulent claims to defraud you. Scammers will ask you for money, personal or financial information, or try to redirect you to sites that require payment or download malicious software onto your computer.

Scams of this sort can be very sophisticated and scammers will go to great lengths to build a relationship with you, spending a lot of time communicating with you and perhaps even telling you they love you and sending you gifts.

The key rule is that you should never send money to anyone you meet online and should reconsider your relationship with anyone who asks you for money or who you otherwise suspect may be a scammer.

Scammers will often ask you to send money via a wire transfer service and you will usually be unable to recover money sent this way. You should also never share personal information, such as bank account or credit card details, as you risk falling victim to fraud and identity theft.

How can I spot a scammer?

Any of the following behaviours should raise concerns that the person you are interacting with is a scammer:

- they claim to be travelling or stationed overseas, even if it is temporary or for work
- they ask you to send them money or provide your personal or financial details
- they ask you to transfer money via a wire transfer service
- they ask you to send larger amounts via a bank transfer
- they quickly profess strong feelings or love for you
- they are vague about their interests, or what they want in a partner and not particular about how old their partner might be
- their computer camera or Skype connection never seem to work
- they do not answer your questions or their responses are formulaic, nonsensical or repetitive
- their profile is at odds with their story, or their communications with you display poor spelling or grammar.

You should carefully consider your relationship with anyone who asks you to move communications with them away from the dating site onto email, instant messaging, the phone, VoIP or some other medium after only a few contacts. Scammers will often ask you to do this so that you will be communicating only with them, are more likely to reveal personal information and you will not receive safety warnings.

You should never respond to a request for money, personal information or banking details, no matter the reason given.

Do an image search of your admirer to help determine if they really are who they say they are. You can use image search services such as Google or TinEye. These searches will often show instances of other people being scammed using the same photo or reveal that the image you have been given is a picture of someone else.

Google search some of the phrases in emails they have sent you. Often you will find their declarations of love have been used over and over again by scammers.

What should I do if I think I have been scammed?

1: Cease communication

If you think you have been scammed, the first step is to immediately cease communication with the scammer, to avoid losing more money or giving away more personal information. Ignore any attempts by the scammer to communicate with you and take steps to block future communications, e.g. set up rules in your email account and on your mobile phone.

2: Contact site operator

You should report the scammer to the dating site where you first had contact with them, as they may be targeting other users. You should provide the site operator with as much information about the scammer as possible. This may include examples of emails or instant messaging communications received from the scammer and photos, names and addresses, email addresses or phone numbers used by the scammer. It may also be useful to provide details of account numbers of where you have sent money.

3: Contact your financial institution

If you have sent money to the scammer, particularly if you have provided any personal or financial details, you should contact your financial institution and inform them. If you have given the scammer information such as account numbers, credit card numbers or passwords you should immediately change them. If you used a service, such as a money transfer service, to send money to the scammer you should contact the service provider so that they can stop others from sending money to the scammer.

4: Report the scam to the Australian Competition and Consumer Commission (ACCC)

Reporting a scam to the ACCC assists with monitoring scam trends. You can report a scam to the ACCC via the online reporting form on the ACCC's scamwatch website www.scamwatch.gov.au. The details of complaints made to the ACCC will be kept confidential.

5: Contact police

If you have sent money to the scammer, report the matter to the police via the Australian Cybercrime Online Reporting Network (ACORN) at www.acorn.gov.au. If someone attempts to blackmail you, or makes threats of any kind, you should contact the police immediately.

6: Beware of future contact

Scammers will often contact you under new guises to try and get more money from you. They may pretend to be lawyers, government officials or police, often from another country, and claim that they have caught the scammer and need money to recover your losses. You should never send money—the scammers are simply trying to get more out of you.

7: Take steps to protect your personal data

Scammers collect information about you during a scam for identity theft. Take some time to review what information the scammer might know about you and take steps to change this information if required. Information such as passport numbers, bank account details and driver's licence numbers are particularly valuable to scammers. Consider changing your mobile phone number, email address and any social media accounts.

Check your settings on any and all social media accounts and restrict access to friends only. Public access is just that. Anyone can find out very personal information about you including: where you live and work; your patterns and routines; and details about your kids, hobbies and interests.

Specific scenarios

Someone has asked me for money for airline tickets or other travel expenses—is this a scam?

This sounds like a common scam. You should never send money to anyone you meet online. Scammers often promise to visit you, then pocket any money you send them. Don't send money for plane tickets, visas, customs fees or any other travel expenses the scammer claims to have. They may send you copies of their passport, tickets or visa to 'prove' they are coming to visit you—don't believe these stories. Scammers often have access to authentic-looking fake documents.

They claim to be in the military and say they need money for a leave pass—what should I do?

This is another common scam and you should never send money. Scammers claiming to be members of the military will often say they need your money to pay for a leave pass or some other expense so they can visit you. This is just an excuse to get you to pay money. The military does not charge for leave passes.

I've been asked to pay money to a charity or to support a business opportunity—is this a scam?

Scammers will often tell you that money you send them will go to a charity or will be used to support a business venture. This might be anything from oil exploration to gold mining, gemstone sales and more. The scammer might also tell you they can access some kind of treasure or inheritance and say that they need money to recover it, resolve legal issues or get a valuable item through customs. You should not send money. Charities don't solicit donations through dating sites and any stories about great riches are just a ploy to get you to make a scammer rich.

I've been told I need to send money because of an emergency—is this a scam?

A medical, legal or other emergency is a common excuse used by scammers to get at your money. To create a sense of emergency, scammers will often tell you that:

- they or a relative, often a child, is sick or injured (often in a car accident or hit and run) and needs money for medical treatment
- they have been robbed or lost their wallet and need money to pay living expenses, a hotel bill or the police
- they have been arrested or detained by immigration authorities and need money for bribes, visa or customs fees
- they have been kidnapped and need your help to pay the ransom.

These stories are designed to make you feel as if the situation is desperate and to get you to send money without thinking. However, you should never send money to anyone you meet online.

My online dating partner says they can't continue chatting with me unless I send money—what should I do?

You should not send money. Scammers will often claim they need you to send them money or they won't be able to communicate with you in the future. They may say that they need money to access the internet, to purchase a webcam or computer, to pay for a translation service or other living expenses.

I've been asked to transfer money for my online dating partner—should I do it?

You should never agree to transfer money for someone else—this may be money laundering, which is a criminal offence. This may also be an attempt to get you to provide personal information for identity theft.

My online dating partner has sent me a mobile phone/computer/tablet and asked me to send them to a friend overseas—what should I do?

You should never agree to send items that have been sent to you to someone overseas—this may be a form of money laundering through high value products rather than money. It is still a criminal offence.

Attachment D—Advice to scam victims

The ACCC considers that the following advice should be given to online dating site users concerned that they have fallen victim to a scam:

1: Cease communication

If you think you have been scammed, the first step is to immediately cease communication with the scammer, to avoid losing more money or giving away more personal information. Ignore any attempts by the scammer to communicate with you and take steps to block future communications, e.g. set up rules in your email and social media accounts and on your mobile phone. Better still, change your mobile phone number, email address and social media accounts.

2: Contact site operator

You should report the scammer to the dating site where you first had contact with them, as they may be targeting other users. Details of your report will be kept confidential. You should provide the site operator with as much information about the scammer as possible. This may include examples of emails or instant messaging communications received from the scammer and photos, names and addresses, email addresses or phone numbers used by the scammer.

3: Contact your financial institution

If you have sent money to the scammer and particularly if you have provided any personal or financial details, you should contact your financial institution and inform them. If you have given the scammer information such as account numbers, credit card numbers or passwords you should immediately change them. If you used a service, such as a money transfer service or bank to send money to the scammer you should contact the service provider so that they can stop others from sending money to the scammer.

4: Report the scam to the Australian Competition and Consumer Commission (ACCC)

Reporting a scam to the ACCC assists with monitoring scam trends. You can report a scam to the ACCC via the online reporting form on the ACCC's scamwatch website www.scamwatch.gov.au. The details of complaints made to the ACCC will be kept confidential.

5: Contact police

If you have sent money to the scammer, you should report the matter to the police via the Australian Cybercrime Online Reporting Network (ACORN) at www.acorn.gov.au. If someone attempts to blackmail you, or makes threats of any kind, you should contact the police immediately.

6: Beware of future contact

Scammers will often contact you under new guises to try and get more money from you. They may pretend to be lawyers, government officials or police, often from another country, and claim that they have caught the scammer and need money to recover your losses. You should never send money—the scammers are simply trying to get more out of you.

7: Take steps to protect your personal data

Scammers collect information about you during a scam and may use this information for other fraudulent activity. Take some time to review what information the scammer might have about you and take steps to change this information. Information such as passport numbers, bank account details and driver's licence numbers are particularly valuable to scammers. Consider changing your phone number and email address. Also review your social media profile and consider changing or amending your Facebook, Twitter, Skype, Linkedin, Pinterest or other accounts. Ensure your privacy settings are set at the highest level and your accounts are accessible to only those people you know and trust.

The Working Group

The following dating site operators formed the working group which participated in the 2015 review of the guidelines:

- Adult Match Maker—Giga Pty Ltd
- Cupid Media Pty Ltd
- eHarmony
- Oasis Active
- RedHotPie.com.au
- RSVP

The ACCC is grateful to those that participated in the original development of the guidelines and those that contributed to the review.