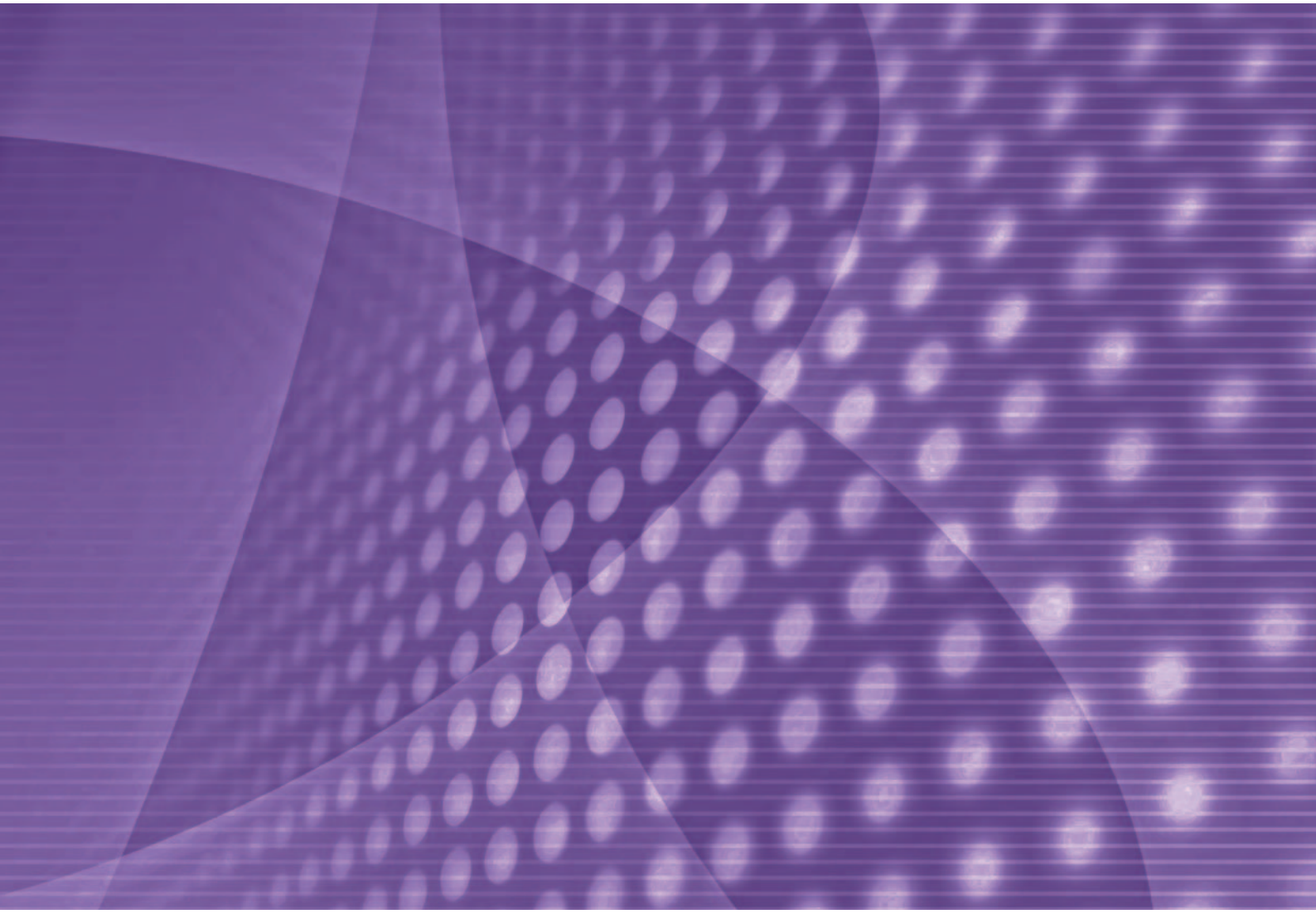

BEST PRACTICE GUIDELINES FOR DATING WEBSITES

—protecting consumers from dating scams

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

Important notice
The information in this publication is for general guidance only. It does not constitute legal or other professional advice, and should not be relied on as a statement of the law in any jurisdiction. Because it is intended only as a general guide, it may contain generalisations. You should obtain professional advice if you have any specific concern.

The ACCC has made every reasonable effort to provide current and accurate information, but it does not make any guarantees regarding the accuracy, currency or completeness of that information.

ISBN 978 1 921964 61 9

ACCC 02/12_45843_472

www.accc.gov.au

Foreword

I am pleased to present the *Best Practice Guidelines for Dating Websites*. These guidelines aim to help dating and romance (D&R) website operators respond to scams targeting their users.

D&R scams are often the work of international criminal networks and cause significant harm to Australian consumers. In 2011, the ACCC received more than 2100 reports of D&R scams and consumers reported more than $21 million in losses to these scams. In 2010, over $15 million in losses were reported. In addition to losing money, many victims of these scams also report serious emotional harm. Similar scams are also targeting Australian consumers through social networking and other websites.

The guidelines have been developed by a working group, chaired by the ACCC and comprising of representatives from a number of dating websites. The contribution of the working group to the development of the guidelines was complemented by consultation with the wider online dating industry.

Many dating websites 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.

One objective of these guidelines is to complement existing measures through key information points, informed complaints handling and ongoing vigilance to identify fake profiles and other scam activities. The other is to provide guidance to those dating websites that are new to the industry or have no such measures in place to enable them to better protect their 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 websites 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 websites and can be tailored to suit the characteristics of their users.

The ACCC recognises and appreciates the contribution of participants in the dating website 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.

Dr Michael Schaper
Deputy Chairman

Contents

Best practice guidelines for dating websites *—protecting consumers from dating scams*

Context

Introduction

1. The Internet and digital technologies are a powerful influence on Australia's economy and society. The online environment also provides opportunities for criminals, including international criminal networks to target Australian consumers.

2. Dating and Romance (**D&R**) websites offer services to facilitate relationships between their members and have become a popular way for people to meet one another. Users of D&R websites can be targeted by scammers who create fake profiles and contact legitimate users for the purposes of fraud. Reported losses by Australian consumers to these scams are very high.

3. Typically, the scammer will form a relationship with a legitimate user, sometimes over a significant period of time, and then defraud them, such as by asking for money or personal information. Victims of these scams often suffer high financial losses, as well as emotional harm.

4. In addition to the significant harm caused to Australian consumers, scam activity may also have a detrimental effect on the online dating and romance business model by undermining consumer confidence in this service. Many D&R websites have already implemented measures to protect their users from scams. It is in the interests of all D&R website operators to act strongly to disrupt the activities of scammers targeting their customers.

5. These best practice guidelines (**the guidelines**) have been developed by the Australian Competition and Consumer Commission (**ACCC**) together with the D&R website industry to bolster the existing measures used by D&R websites to counter the activities of scammers and provide guidance to the industry on how to better inform and protect their users.

6. The actions detailed in the guidelines are divided into three categories:

    6.1 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 D&R websites is attached to these guidelines.

    Consistent messaging across D&R websites may enhance the effectiveness of these warnings. D&R websites can make use of the attached warnings and adapt the wording to suit their individual needs, while retaining the essential message.

    6.2 Vetting and checking system—

    A robust vetting and checking system to identify scammers both as they attempt to register with a website and following registration is an important tool for D&R websites to disrupt the activities of scammers.

    6.3 Complaint handling procedures—

    Effective complaint handling procedures are vital for D&R websites to respond to scams. They allow for scammers to be quickly identified and action taken to protect users. Such procedures must be easily accessible to users, responsive to their complaints, and informative.

Scope

7. These guidelines are suitable for adoption by all D&R websites that are used by Australian consumers, whether they are based in Australia or overseas.

Objective

8. These guidelines seek to protect Australian consumers by providing a set of actions for implementation by D&R website operators to improve their response to scams.
9. These guidelines are voluntary and are intended to represent best practice.
10. All D&R website operators should implement the actions contained in the guideline, supplemented by any additional actions they identify as effective.
11. 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 D&R website.
12. The attachments to the guidelines provide material which may be used by D&R website operators for warning messages and to inform their users about scams.
13. 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 websites 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

14. In order to educate and inform their users, D&R websites should provide information and warning messages about scams. Warning messages should include both key messages and examples in appropriate locations.

Display of warning messages

15. Warning messages should be clearly and prominently displayed at appropriate locations on the D&R website in a form likely to be noticed and make an impact on users, such as a banner, sidebar, insert or link to further information.

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

17. For example, warning messages may be displayed:

    17.1 where members communicate including chat, instant messaging, email and other communication services provided by the website

    17.2 at any other relevant locations frequently visited by website users.

Content of warning messages

18. As part of their warning messages, D&R websites should display key messages to warn their users about the risk of scams.

    18.1 To be most effective, key messages should be simple and direct.

    18.2 Key messages should be appropriate to the area of the website on which they appear.

19. A set of example key messages for use by D&R websites is at **Attachment A**. Use of these example messages will reinforce the consistency of warnings across the industry. However, websites can also adapt the exact wording and location of these messages to suit their layout and the needs of their user base.

20. D&R websites may also develop additional key messages which they consider effective. These messages should also be simple, direct and consistent with those in Attachment A.

21. In addition to key messages, D&R websites should also display 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.

    21.1 Examples may be displayed in a brief format in the same locations as key messages, or with more detail elsewhere on the website.

    21.2 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.

22. A set of examples of scammer conduct is at **Attachment B.** However, websites can also adapt the exact wording of these examples to suit their layout and the needs of their user base.

23. D&R websites are encouraged to develop additional examples based on their own experience of scams.

24. D&R websites should also regularly review their examples to ensure they reflect current trends in scammer behaviour and to warn users about new and emerging scams.

25. 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 rotating set of such messages.

Provision of detailed information

26. D&R websites should provide their users with access to detailed information on scams. This information may be provided as part of the website, or on a separate dedicated online safety page.

27. The attention of users should be drawn to this information. For example, the information or a link to the information could be provided:

    27.1 as part of information on how to use the websites 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

    27.2 during regular communications with members—such as a newsletter or update service

    27.3 through links within the D&R website where appropriate.

28. D&R websites may also display a link to scam information on their homepage.

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

30. This information may include:

    30.1 warning signs when a user is communicating with a scammer

    30.2 common stories used by scammers when they request money

    30.3 steps to be taken if a user thinks they have fallen victim to a scam (see paragraph 44 below)

    30.4 any other information relevant to educating users about scams.

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

32. D&R websites may provide a link to the ACCC's SCAMwatch website (www.scamwatch.gov.au), which contains information about a variety of scams, including D&R scams, but website operators should also maintain information about D&R scams on their own website.

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

Mobile websites and Smartphone applications

34. In addition to websites accessed via a computer and internet browser, some D&R websites maintain versions of their site optimised for viewing on a mobile phone (mobile websites) and/or offer applications ('apps') for use with a Smartphone or other device.

35. D&R websites should display simplified scam warnings and/or prominent links to information on scams on websites or apps designed for mobile devices as appropriate and in keeping with the objective of the guidelines.

Vetting and checking system

36. While it may not be possible to identify all scammers, D&R websites should implement a robust vetting and checking system intended to identify scammers as they attempt to register with the website and following registration.

37. A robust vetting and checking system should 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 website.

38. For example, characteristics which may be checked by such a system include:
    - 38.1 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
    - 38.2 checking of profile pictures, to identify common pictures used by scammers
    - 38.3 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
    - 38.4 measures to address the use of proxy servers and other methods to evade IP checking
    - 38.5 abnormal behaviour by users within the website, such as the volume of messages sent or responded to
    - 38.6 any other characteristics which are an effective way to identify profiles likely to be created by scammers.
39. D&R websites should adopt a vetting and checking system that best fits their website structure and level of traffic. Such a system can involve manual or automated checks, or a combination of both.
40. As the methods used by scammers may change over time, D&R websites should regularly review their vetting and checking system to ensure it remains effective.

Complaint handling procedures

41. In order to identify scams, gather information and assist affected users, D&R websites should provide complaint handling procedures where users can report a scam and ensure users are aware of this system.

Lodging a complaint

42. D&R websites should set up mechanisms for users to report suspicious conduct within the D&R website—such as a button entitled 'report a scam', 'report abuse' or other words to similar effect.
43. 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

44. D&R websites should implement the following referral process for Australian users who have identified or been affected by a scam:
    - 44.1 advise users to report the scammer to the website operator first
    - 44.2 advise users they can report the scam to the ACCC SCAMwatch website—www.scamwatch.gov.au
    - 44.3 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
    - 44.4 advise users who have lost money to a scammer, or where the scammer has threatened or attempted to blackmail them to contact their state or territory police force.
45. A template advice to users on what to do if they have fallen victim of a scam is at **Attachment D**.
46. Non-Australian users who report a scam should be referred to their local consumer protection and legal authorities as appropriate.
47. As legitimate users may lose access to the website if their profile is hacked or mistakenly removed, D&R website operators should ensure that their customer service staff can be contacted via an alternative that does not require the user to be logged in.

Responding to complaints

48. Where the user seeks a response, D&R website operators should 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 should take if they have fallen victim to a scam.

49. Upon receipt of a complaint about scam activity, D&R website operators should investigate the profile alleged to be engaging in scam activity and take appropriate action as soon as possible.

50. Where a profile has been identified as a scammer, the website operator should notify other users contacted by that scammer.

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

52. D&R websites should keep the details of customer complaints confidential and advise their customers that they will do so.

53. D&R website operators should collect data on complaints about scams in order to monitor the effectiveness of their anti-scam measures and update them when necessary.

    53.1 This data would include the number of complaints, the amount of money reported lost and the type of scam.

    53.2 The data is to be collected from the information provided by the complainant. It does not require D&R websites to seek further information from complainants.

Attachment A—Key messages

- Never send money to anyone you meet online
- 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
- Don't share your banking or credit card details with anyone you meet online
- If someone asks you to transfer money to them via a wire service, don't do it
- If someone asks to move your communications outside the website 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
- If someone offers to send you money orders to cash on their behalf, don't do it—you may be defrauded

Attachment B—Examples of scammer conduct

The ACCC considers that the following could be used by D&R website 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 for 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'

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

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

'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 have been stationed in Africa as an oil worker, aid worker 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 or for 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 fraud.'

'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 recent 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.’

Detailed example of scam progression

Jessica, an Australian businesswoman in her forties, met a man called Martin on an online dating website.

Martin’s profile said that he was an Australian stationed in Ghana as an aid worker. 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.

Soon after getting in touch, Martin told Jessica that he could not reliably access the dating website from Ghana 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.

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. The phone calls were the worst because he knew how to push all the right buttons. She should have hung up straight away but she still felt something for him.

Jessica felt devastated that a man she had been sharing so much of herself with for so long and felt she could trust implicitly had been 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 FAQ

What is a dating scam?

On a dating website, a scammer is someone who builds a relationship with you, pretending to be a legitimate user of a dating website, and then uses fraudulent claims to defraud you. Scammers will ask you for money, personal or financial information, or try to redirect you to websites 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 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 quickly profess strong feelings or love for you
- they are vague about their interests, or what they want in a partner
- they do not answer your questions or their responses are formulaic, nonsensical or repetitive
- they claim to be stationed in or travel frequently to Africa or elsewhere overseas
- their profile, 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 website 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 will not receive safety warnings.

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

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.

2: Contact website operator

You should report the scammer to the dating website where you first contacted them, as they may be targeting other users. You should provide the website 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, to send money to the scammer you should contact the service provider.

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 contact your state or territory police and report your loss. 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.

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.

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 websites 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.

Attachment D—Advice to scam victims

The ACCC considers that the following advice should be given to D&R website 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.

2: Contact website operator

You should report the scammer to the dating website where you first contacted them, as they may be targeting other users. Details of your report will be kept confidential. You should provide the website 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 to send money to the scammer you should contact the service provider.

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 contact your state or territory police and report your loss. 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.

The Working Group

The following dating website operators formed the working group which developed the guidelines. The ACCC is grateful for their substantial contribution to the success of this project.

Adult Match Maker—Giga Pty Ltd
Cupid Media Pty Ltd
Ezifriends
Oasis Active
Pink Sofa Ltd
RedHotPie.com.au
RSVP
Rural Romeos
Slinky Dating Australia Ltd