“I Suspect That the Pictures Are Stolen”: Romance Fraud, Identity Crime, and Responding to Suspicions of Inauthentic Identities

Cassandra Cross¹,² and Rebecca Layt²

Abstract
Romance fraud impacts the lives of thousands of people globally. Financial losses exceed millions of dollars each year and are steadily increasing annually. It occurs when an offender uses the guise of an intimate relationship to gain a financial advantage. Offenders use a variety of platforms and communications methods to target victims and develop the required trust and rapport to defraud them. As part of this process, offenders use false identities. This can be through the misappropriation of a genuine person’s identity, or it can be through the stealing of photos and other images of a genuine person to create a false or fictitious identity. In this way, romance fraud encompasses two categories of victims: those who lose money through a relationship and those who are subject to identity crime by romance fraud offenders. This article examines how individuals responded to suspicions of inauthentic identities to a person they were communicating with online. It uses romance fraud complaints lodged with Scamwatch (an Australian online fraud porting portal) between July 2018 and July 2019 (inclusive). The qualitative analysis indicates that many complainants used an internet search to verify or refute their suspicions about their partner. This yielded substantiated results in many cases and confirmed that the offender’s identity was not genuine. The article explores the implications for this victim-based detection strategy. In doing this, it argues that while effective for romance fraud victims, responses can further exacerbate the ongoing harms experienced by those whose identities have been compromised by romance fraud offenders. The article concludes with a discussion about the future effectiveness of internet searches to reduce romance fraud and the impact of this strategy on third parties whose identities are compromised by offenders.

Keywords
romance fraud, identity crime, inauthentic identity, deception, online dating

¹ Cybersecurity Cooperative Research Centre, Queensland University of Technology, Brisbane City, Queensland, Australia
² School of Justice, Queensland University of Technology, Brisbane City, Queensland, Australia

Corresponding Author:
Cassandra Cross, Cybersecurity Cooperative Research Centre, Queensland University of Technology; School of Justice, Queensland University of Technology, 2 George St., Brisbane City, Queensland 4000, Australia.
Email: ca.cross@qut.edu.au
Romance fraud devastates the lives of thousands globally. The Internet Crime Complaint Centre (IC3) noted that in 2019, romance fraud was in the top three fraud categories for financial loss, with over US$475 million reported (IC3, 2020). Substantial losses are also evident in other countries with Australians reporting losses of over AUD$80 million in the same year (Australian Competition and Consumer Commission [ACCC], 2020), and the British reporting over £50 million lost in 2018 (Peachey, 2019).

Romance fraud (also known as dating and relationship fraud) occurs “where a person is defrauded by an offender/s through what the victim perceives to be a genuine relationship” (Cross et al., 2018, p. 1304). A key element to perpetration of romance fraud is the use of identity crime. Unsurprisingly, offenders do not use their own personal profiles in their attempts to defraud individuals. Rather, the offender will create their own fake profile (often using legitimate photos of a different person) or take on the profile and identity of a genuine person. In these instances, the offenders are not only perpetrating romance fraud, but they are also committing identity crime.

There is a complex relationship between romance fraud and identity crime. In an online environment, it is difficult to establish the authenticity of a person’s identity. The nature of online communication removes many of the visual cues relied upon and places a stronger emphasis on words and pictures (Steel, 2010). This can have dire consequences for victims who are unable to discern the fraudulent nature of requests and scenarios presented to them.

In many of these cases, victimization not only extends to the individual who may have sent money but also extends to those whose identities have been assumed by an offender. While the deception surrounding the use of identity crime is integral to the perpetration of romance fraud (Cross, 2020b), there is no known research that explicitly looks the ways in which those targeted by romance fraud are confronted by the potential inauthenticity of profiles, and how they seek to verify the identity of the person they are communicating with online. There is also no consideration as to those individuals who experience identity crime at the hands of romance fraud offenders. It is this gap that the current article seeks to explore.

This article examines the ways in which individuals reporting romance fraud were confronted with the possibility of inauthentic identities of a person they were communicating with online. Based on 2,671 reports made to Scamwatch (an Australian online reporting mechanism for fraud) between July 2018 and July 2019 (inclusive), the article examines a subset of reports (n = 509) which detailed their responses to suspicions of inauthentic identities.

To achieve this, the article is as follows. First, an overview of romance fraud and identity crime is given to locate the context of the research. Second, the methodology used for the analysis is outlined. Third, the results of the data are presented. This provides an overview of the actions taken by individuals in response to their suspicion and reveals two main courses of action: an internet search and/or seeking assistance from third parties.

The article then moves into a discussion locating these results in the context of current prevention messaging regarding romance fraud. It also highlights tensions in the effective use of internet searches as a way of identifying fraud without further victimizing those third parties subjected to identity crime. Finally, the article considers how offenders may use artificial intelligence (AI) to overcome the effectiveness of internet searches currently used by those targeted.

Overall, this article argues that current prevention messaging regarding the searching of images can be an effective way of discerning the authenticity of someone’s online identity, to guard against romance fraud. However, there is a need to think about how this can evolve with technological advancements in the near future, as well as consider a means of achieving this without perpetuating ongoing harms of identity crime on third parties (such as those who have their identities stolen). There is also recognition of the value of third parties in being able to assist with determining potential fraud victimization; however, this is tempered knowing the high levels of victim blaming that exist for this type of victim.
Romance Fraud

Romance fraud “is a method used by offenders whereby they use the perception of a legitimate relationship in order to manipulate and exploit the victim” (Cross, 2020b, p. 3; see also Whitty, 2013). This can be differentiated from a “bad relationship” through the modus operandi of the offender who has created this identity and initiated contact with the potential victim with the express intent of gaining a financial advantage (Cross et al., 2018). In most cases, romance fraud leads to a loss of victim finances. However, there are also a range of nonfinancial harms (Button et al., 2009, 2014b; Cross et al., 2016) as well as the “double hit” of victimization, where victims must grieve both the loss of the relationship in addition to any monetary loss (Whitty & Buchanan, 2012).

Offenders perpetrate romance fraud through many communication platforms. Online dating websites are popular ways of connecting with potential victims, but there has also been an increase in offenders using other social media platforms and apps, such as Facebook, Instagram, and games such as Words with Friends (ACCC, 2020, p. 11). Offenders will seek to develop trust and rapport with the victim, through constant communication through a variety of channels (such as email, text messaging, phone calls, and video calls; Cross et al., 2016). As with all fraud, the ultimate goal of the offender is financial gain (Fletcher, 2007). This is usually through the direct transfer of money but can also come indirectly through the gaining of personal information and identity credentials to perpetrate identity crimes. Offenders are able to achieve this through the use of social engineering techniques (Drew & Cross, 2013) as well as through psychological abuse tactics (Cross et al., 2018).

The research indicates that during the relationship, victims may start to question the authenticity of the offender’s identity and the context in which financial requests are being made (Cross et al., 2016). As stated earlier, offenders are generally not using their own identities. Rather, they have taken on the identity of a genuine person or created a false identity through the misappropriation of another person’s details or photos.

Identity Crime

Identity crime is one of the most pressing and growing crime types of recent decades (Berg, 2011; Holt & Turner, 2012; Pontell, 2002). Identity crime can be understood as an “umbrella concept” (Wall, 2013, p. 437) that includes “identity theft, identity fraud, identity fabrication, identity manipulation, [and] lent identities” (Smith, 2011, p. 142). Similarly, false identities are argued to be established in the following ways: the creation of a fictitious identity (identity fabrication), the alteration of one’s own identity (identity manipulation), or the theft or assumption of a preexisting identity (identity theft which may also involve subsequent manipulation; Australasian Centre for Policing Research [ACPR], 2006, p. 7). However, the nature of these different categories in the literature is disputed as well as to how they interact with each other (Steel, 2010).

Identity theft can be defined as “the unlawful use of another’s personal identifying information” with personal information being understood to “include the individual’s name, address, social security number, date of birth, alien registration number, driver’s licence information, mother’s maiden name, or biometric information such as a fingerprint, voice print, or retina image” (Allison et al., 2005, p. 19). Identity fraud “generally involves a person falsely representing himself or herself as either another person or a fictitious person” (Pontell, 2002, p. 306), in order to obtain “money, goods, services or other benefits through the use of a false identity” (ACPR, 2006, p. 9).

While identity fraud and identity theft appear somewhat interchangeably in some of the literature (ACPR, 2006; Berg, 2011; Lynch, 2005), there is some agreement on the interconnectedness of both identity theft and identity fraud. Vieraitis and colleagues (2015, p. 15) argue that “identity theft involves two separate elements, the theft of information and the fraudulent use of that information.” In a similar vein, Steel (2010, p. 52) notes that “a victim of identity theft loses nothing when their
identity is appropriated. Any loss that occurs is instead associated with the illegitimate use to which their copied identity is subsequently put.” While the use of false identities and identity crime is used by offenders across a range of offenses, “it is most commonly linked to fraud” (ACPR, 2006, p. 7).

The scope of identity crime and its prevalence is difficult to establish for several reasons. Piquero and colleagues (2011, pp. 438–439) assert that,

The true incidence of identity theft remains difficult to capture because of the various definitions of identity theft, the lack of understanding of the techniques used to commit identity theft, and the “unknown victimisations” and/or lack of reporting by victims to appropriate authorities.

A further challenge is the likelihood that victims of identity crime may not be aware that anything has occurred (Seda, 2014, p. 461)

The impact of identity crimes, across both identity theft and identity fraud, can be severe. There is a growing body of research which documents the negative impacts of identity crime on the physical and psychological well-being of victims (Albrecht et al., 2011; Berg, 2011; Burns & Roberts, 2013; Milne, 2003). In addition, victims of identity crimes may face a range of consequences such as incurring financial liabilities, credit-related consequences; and reputational damage, criminal justice consequences (false arrest), and loss of time in seeking to repair the damage done to one’s identity (Albrecht et al., 2011; Berg, 2011; Burns & Roberts, 2013; Button et al., 2014a; Jorna et al., 2020; Milne, 2003).

While identity crime is not a new offense, the evolution of technologies and the internet has enabled offenders to perpetrate these acts on a much larger scale (Pontell, 2002) and target a greater number of victims (Piquero et al., 2011). The ability of offenders to access and misappropriate identity information from a victim is largely effortless, with many individuals posting large amounts of details on a variety of social media platforms as well as the increasing number of data breaches that expose and compromise sensitive and personal information.

The Relationship Between Romance Fraud and Identity Crime

With regard to romance fraud, offenders embrace the use of online deception to attract potential victims and develop a personal relationship. Online deception can be defined as “a broad set of malicious practices that use the Internet as a medium to intentionally give a target (receiver or victim) an incorrect mental representation of the circumstances of a social exchange” (Chen & Huang, 2011, p. 94). In the context of romance fraud, the online deception manifests itself in false identities and corresponding narratives to accompany the false identity. While there has been no specific research which explores identity crime in the context of romance fraud, the likelihood of becoming a victim of identity crime (or having one’s photo or identity used by an offender to defraud another victim) may not be the same for all individuals. Anderson (2006, p. 161) argues the following,

A person does not do something to become a victim, it just happens. However, deeper reflection suggests that this is not the case. Indeed, the risks faced by consumers differ, and these differences may manifest across groups with different demographic characteristics.

In the case of romance fraud, there is anecdotal evidence to suggest that offenders select particular types of identities; ones that they believe will be the most successful in allowing them to attract and connect with potential victims. An example of this is the use of a military profile. Offenders will often employ a military identity and narrative to both capture the attention of a potential victim and then to justify subsequent financial requests (Cross & Holt, 2021). A military identity implies several positive attributes in an individual such as honor, courage, trustworthiness, and loyalty, and
offenders will use these profiles to increase their chances of establishing a successful connection. Further to the military profile, there is also a common adoption of professional occupations such as lawyers, doctors, and engineers (Chang & Chong, 2010; Nhan et al., 2009). In combination, offenders are likely seeking to harness the power and status of an identity to conduct their offending.

The online nature of communications in developing a relationship also provides challenges to the verification of one’s identity. For example, “physical cues, such as nervousness, ability to speak the language, as well as age and gender can all be more easily disguised in a largely text based form of identity” (Steel, 2010, p. 49). There is also the existence of what scholars have termed “hyperpersonal relationships,” whereby technology facilitates the development of relationships more intensely and quickly than their offline counterparts (Jiang et al., 2011; Walther et al., 2015; Walther, 1996). This provides a fertile context for romance fraud offenders to use both genuine or fictional identities to target and defraud their victims.

Method

To date, there is no known research which has explicitly examined how individuals navigate suspicions when confronted with the possibility of inauthentic identities in the context of romance fraud. Further, there is no research which considers the impact of identity crime on third parties who find their personal details have been misappropriated by a romance fraud offender. It is this gap that the current article contributes toward. To do this, the article addresses the following research questions:

**Research Question 1:** What actions do individuals take in response to suspicions of inauthentic identities?

**Research Question 2:** How can this knowledge be used to improve future prevention messaging?

To answer these questions, a qualitative analysis was undertaken using reports of romance fraud lodged to the ACCC. A description of the dataset used is provided below.

Data

The data for this analysis were obtained from the ACCC. The ACCC is a federal government body whose main ambit is consumer protection. They host the Scamwatch website and reporting portal, releasing an annual publication detailing the number of fraud reports received and noting latest trends. While the ACCC has some powers regarding matters of consumer protection, they do not have the power or authority to investigate individual fraud complaints. Rather, they work tirelessly on education and awareness with some focus on disruption activities in collaboration with relevant parties (Scamwatch, n.d.).

Based on their hosting of the Scamwatch website, a request was submitted to the ACCC for data relating to romance fraud reports. An ethics exemption was granted by Queensland University of Technology Human Research Ethics Committee (#1900000738) for this data. In response, the ACCC provided data for those who had reported romance fraud to Scamwatch during the period July 1, 2018, and July 31, 2019 (inclusive). While targeted at Australian victims, the online nature of the portal means that victims across the globe can lodge a report on an incident which may or may not have an alleged Australian link. There were 4,354 reports filed during this time frame, with 3,463 (80%) reports indicating that they were willing to share the contents of their report for scam awareness. It is important to note that Scamwatch is not a law enforcement agency and cannot investigate or take action on individual fraud complaints. Rather, the information gathered by
Scamwatch is used for intelligence purposes to drive consumer awareness and education across Australia.

The ACCC provided a de-identified excel spreadsheet containing the details of these 3,463 reports. Each report included the following information: demographic details of the complainant (gender, age, and jurisdiction both within Australia and overseas), details about the fraud (how the approach was received, the location of the alleged offender), and any losses incurred (amount, payment methods, sensitive details lost). Vulnerability indicators of the complainant were also included, particularly around age, disability, sickness, financial hardship, and location. Importantly, the de-identified free text field where each complainant could write a summary/description of what happened was also made available.

Upon review of the data, 204 duplicate entries were removed, leaving a final total of 3,259 distinct reports available for analysis. Of these, this article focuses on an analysis of 2,671 reports that were categorized as relating to online dating. The other 588 were excluded as they focused on account issues (such as billing and subscription issues to dating websites); related to real life incidents (relationships where it was clear that the persons were in direct contact with each other physically); or were primarily sextortion reports (where a complainant was threatened with exposure of an intimate picture/recording if money was not paid). These three types of romance fraud reports were excluded as they are argued to have a different modus operandi to many of the other romance fraud reports, where communication is established online and leads to (or attempts to lead toward) the development of a perceived relationship in order to obtain financial advantage. Further, the sextortion reports were qualitatively different, in that the focus of the report was on the circumstances that led to the taking of intimate images and the threat to expose them rather than details relating to identity in any way.

Of the 2,671 in the final sample, 509 (19%) distinct reports contained details in the free text section relating to the possible inauthenticity of a person they were communicating with online. The 509 reports which made some reference to suspicions of identity were cut and pasted into a new excel spreadsheet and subsequently imported into NVivo version 12 (qualitative computer-assisted software analysis tool). Once in NVivo, the free text comments were initially coded against three themes: comments that related to the identity of the potential offender, comments that related to the identity of the complainant themselves, and comments that related to the identity of a third party. In this way, a deductive coding approach was taken, whereby the free text narratives were coded against these predetermined categories. Any comment that made reference to being suspicious of the identity of the person they were communicating with was coded under the node “identity of the offender.” Any comment that made reference to aspects of their own identity (such as details of personal information they had shared during their communications) was coded under the node “identity of the complainant.” Finally, any comment that related to the identity of the third party used by the person they were communicating with was coded under the node “identity of a third party.” Some reports contained comments which crossed these three nodes.

Once in these three nodes, an inductive approach was used to explore how comments related to identity were presented. In doing this, it became clear that complainants took specific action in response to a suspicion of authenticity. Consequently, the “identity of an offender” node was further coded into the actions that complainants took (internet searches and seeking assistance from third parties) and whether this search was substantiated (found evidence to support a suspicion) or unsubstantiated (was not able to find evidence to support a suspicion). It is these data and coding that the current article is based upon.

There was a degree of difference in the quality and content provided by complainants across the free text fields in each of the reports. Some complainants entered brief phrases or statements which related to the questioning of a person’s identity. In contrast, other reports contained long and detailed descriptions or summaries of what had occurred, which included a greater level of detail on their
suspicions relating to the identity of the offender and the actions they took in response to this. However, it is important to note that the length of the free text narrative did not necessarily equate to better data. For some, the short description contained all that was needed to ascertain suspicions of identity, whereas other reports contained lengthy descriptions containing a large amount of tangential detail.

The following results include limited statistics for the numbers of reports across particular themes. However, these should be interpreted with caution. The following analysis simply reflects what was available in the current data set. Some complainants may have had suspicions but not articulated in the free text field of their report. Therefore, it represents only what the individual complainants chose to share when reporting to the Scamwatch portal. Given the free text field was not mandatory, and there were no prompts requiring an assessment on the identity of the offender, the prevalence of the themes examined in this article may be much higher than what is currently reflected. Nevertheless, the reports analyzed within this article provide important insights into how individuals navigated the potential inauthenticity of profiles and their actions taken in response to their suspicion. It is also important to note that those who wrote about the potential for inauthenticity throughout communication included those who lost money, those who lost sensitive information, those who lost both money and sensitive information, and those who did not suffer either of the above. For the purposes of the current analysis, these groups have not been differentiated.

Navigating the Potential for Inauthenticity in Communications and Relationships

The following section begins to detail the ways in which complainants articulated and responded to a suspicion of the inauthenticity of the identity of the person they were communicating with online. Specifically, it focuses on the actions to verify or mitigate against the suspicion of an inauthentic identity.

Actions Taken to Verify or Mitigate Suspicions

When confronted with the possibility that the identity of the person they were communicating with online may not be authentic, many complainants detailed a course of action taken to verify or mitigate these suspicions. There were only two courses of action that were presented in the data. The first was the use of an internet search, and the second was seeking help from a third party. Both of these are examined.

Internet searches. Of the 509 reports in the current analysis, nearly one half \((n = 239)\) took this action to assist them with their decision making. In doing this, complainants reported both success and failure from doing an internet search, and how this process did or did not assist with confirming or rejecting their suspicions.

There were many complainants \((n = 172)\) who indicated that they had done a reverse image search through a search engine (such as Google). In many cases, this search produced results which led them to the realization that the person they were communicating with was not the person they had portrayed themselves to be. For some, the person had multiple profiles across a variety of social media platforms, with a variety of names.

I did a google search on his photo comes up heaps of times with different names and countries. (Case 2064)

So I search the soldier picture on google and was surprised to discover he was a scammer using different names. (Case 2635)
For others, they found what they perceived to be the “real” identity behind the person they were communicating with online.

This person is impersonating an Army Sergeant Major of the USA having obtained pictures from the internet & created this fake profile. (Case 1922)

I receive several messages from him, but I felt a bit weird so I checked his photo and found completely different profile with the same photo at twitter. (Case 1945)

In several cases, the pictures used by the offender were those of a celebrity or well-known identity. Upon finding this, it immediately cast doubt as to the authenticity of the profile.

I Google reverse his photos he sent to me... finds out it was taken or copied from Instagram of [redacted] an actor and a singer. (Case 2396)

I had done a Google image search he is using... New Zealand [politician] [redacted] picture as his profile picture. (Case 242)

As well as finding celebrity identities, there were several complainants (n=54) whose search led to the picture or profile being highlighted on a website as fraudulent. This is highlighted below.

This time I was a step ahead of him. Once he told me that he was deployed I already knew where it was going. Sure enough I checked the scam picture web page and ALL of the photos he used are on there. (Case 399)

And the same day I checked his photo for scammers. HE IS THERE. (Case 3159)

It is clear that the ability of individuals to reverse search images sent by an offender is a useful step for many to realize the inauthenticity of the person they are communicating with online. Internet searches were not just relegated to images. Complainants (n = 44) also indicated a range of other factors which they searched. This included addresses, phone numbers, personal details, and the content of messages used by the offender. A selection of these are illustrated below.

He gave me an address and I googled it and it was a middle of the intersection so I called the post department and they said that address did not exist. (Case 786)

They then send a copy of the passport as “proof” and it is all wrong. I google the serial number for the passport and it is reported as fake. (Case 737)

Did a background check on list of authorized building contractors in [state] and the company name and person doesn’t come close. (Case 2373)

However, not all internet searches were able to assist the complainant in determining the authenticity of the identity or the story they were being told. In some circumstances (n = 31), complainants were not able to find anything. Again, the use of reverse image searches was evident (n = 15). In each of these cases, the search did not yield any matches on the internet.

I did a reverse image search on his photos and they don’t appear anywhere online. (Case 59)

I suspect him [to be] a scammer. But I not sure because I Google his picture couldn’t find anything. (Case 872)

Similar to above, there were also complainants who were hoping to find details on a website warning about fraud.
When I felt he was fake I put his pictures in Google search and Tin eye checked some of those Scam sights [sic] and nothing came up at all. (Case 627)

I suspect that the pictures are stolen but I didn’t foud [sic] any information on scammer pages. (Case 509)

As well as not being able to find any pictures, there were a small number of individuals \( n = 13 \) whose search did not return any details of the identity at all. This added to the unease already being experienced.

I’ve been googleling [sic] him since and I can’t find any real information. (Case 525)
I have searched Facebook and google but can’t find any information on him anywhere—eg like he doesn’t exist in the real world. (Case 3292)

A lack of information did not necessarily give the complainant peace of mind or reassurance about the authenticity of the identity. This is highlighted below.

Nice photo of the person which I have done a check on and have had no matches through google. If this is genuine then I’d be pleasantly surprised but the facts don’t add up. (Case 938)
Too many strange things. Plus I can’t find him anywhere by the name and address he gave me...I believe he is a scammer. (Case 2365)

In combination, these reports indicate that the main course of action taken was the use of an internet search, albeit with varying degrees of success with the results.

Seeking assistance from a third party. In a small number of cases \( n = 23 \), complainants reported that they had sought assistance from a third party in response to a suspicion of inauthentic identities. However, it was evident that in many of these circumstances, the third party (family member or friend) still used an internet search to verify or refute an inauthentic identity. This is demonstrated below.

Early January I gave to my friend all the websites he [offender] used for her to check such as [redacted], all pictures he sent all are fake webs & pics. (Case 1706)
My daughter helped show me the sight [sic] that can show of [sic] a picture has been edited and the first one we downloaded was the one where his head was slotted over the top of someone else’s and that was when it hit me the total betrayal of this man. (Case 3379)

There were only a few examples, where it was evident that the complainant had sought to make direct contact with third parties in response to their suspicions. This came in the form of formal organizations (banks, consulates, government departments) and was to check on the validity of either personal details provided or documents which had been sent.

I contacted the [redacted] department he claimed the email and letter were from and they verified the documents are a scam. (Case 634)
I got suspicious and investigated from my end with [organisation] who emailed confirming that he does not work for them and they never need to ask for money when volunteering. (Case 104)

In two cases, complainants indicated that they had engaged a private investigator to determine the authenticity of the person they were communicating with.

Ultimately I googled a private investigator in Paris paid him $40.0 gave him a copy of her French ID that she gave me and other relevant information. He came back with a report showing the ID was fake and no
trace of her in France. I sent this to her and she called the P.I. a liar and I haven’t heard from her since. (Case 1312)

I engaged an American investigator to find this person and they concluded that this person’s address, phone number, personal details and email addresses were all fake. (Case 2793)

In this way, the reports indicate limited use of offline techniques to determine the authenticity of the person they were communicating with. Unlike the previous section, all reports which mentioned the use of a third party indicated that they had been able to refute the authenticity of the identity as an outcome.

**Summary of Actions Taken**

Overall, this section has demonstrated how complainants used both internet searches and third parties to verify or refute their suspicions of inauthentic identities. In many cases, the internet search was able to support their suspicion and provided evidence that the identity was not genuine, particularly through the use of reverse image searches. However, there were also other elements to the story which were able to be refuted through a simple internet search. Further, complainants looked for warnings on dedicated fraud and scam websites that matched their circumstance. In contrast, there were a smaller number of individuals who did not find any evidence to support their suspicion, either through a reverse image search or a more general internet search (including scam websites). The inability to find any details of the person was equally as likely to lead to a determination that the person was not genuine.

There were a smaller number of complainants who sought assistance offline, from third parties. This included informal networks of family and friends but also encompassed formal networks across organizations and private investigators. In these circumstances, complainants indicated consistent success in being able to establish the deception of the identity they were communicating with.

**Discussion**

Online mediums change the ways in which individuals communicate (Schlosser, 2020). In the context of relationships, it provides many challenges in terms of being able to verify and authenticate the true identity of a person that one is communicating with online, so there is a risk of experiencing both lies and deceit (Couch et al., 2012). With the removal of physical and visual cues, communication relies heavily on the written word as well as photos and documents sent by one person to another (Steel, 2010). In the context of romance fraud, offenders will do whatever is necessary to build trust and rapport with a potential victim, and, to accomplish this, they use a range of techniques (Cross & Kelly, 2016).

The above excerpts from complainants’ romance fraud reports provide a unique foundation for thinking about current prevention messaging regarding online identities as well as ways to educate individuals on what to do in the event that they have suspicions on the authenticity of the person they are communicating with online. Further, there are also implications for responding to and supporting those who are victims of identity crime, through an offender using their personal information (such as names or photos) to commit fraud. The current methods of seeking to prevent romance fraud victimization and help individuals confirm an offender have implications in perpetuating the victimization of identity crime victims. Both areas will be considered in greater detail below.
The Power of an Internet Search

It is evident from the data that many complainants used the internet to search for evidence to either support or refute the details they were given about the person they were communicating with online. For most, this involved a reverse image search of a profile picture or another picture that an offender had sent. Complainants used different search engines to do conduct this investigation and used a combination of social media and other websites. This action matches with current prevention messaging that exists with regard to protecting against romance fraud. For example, on the Australian Scamwatch website, it specifically states “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” (Scamwatch, n.d.). The same advice is promoted by other agencies across the globe who also work against romance fraud, such as the USA’s Federal Trade Commission and New Zealand’s Netsafe (FTC, n.d.; Netsafe, n.d.). This is also a technique used in the popular television series *Catfish* (MTV, 2020).

For the many who undertook this action, suspicions were substantiated, in that the complainant found that their image was on the internet, either attributed to another identity (in some cases, multiple identities) or attributed to a known romance fraud offender. This demonstrates the awareness that several complainants had to take this action as well as the relevant effectiveness of this prevention strategy in seeking to determine the authenticity of someone online. Even for those complainants who were not able to find the photo online, in many cases, they still used this unsubstantiated search result to confirm their suspicion about the authenticity of the person they were communicating with online.

The notion of an individual’s “digital footprint” or “the body of information that exists on the internet as a result of online activity relating to them” (Anonymous, 2019, p. 14) is a new concept that recognizes the scope of one’s online interactions. The emergence and subsequent dominance of social media platforms has “become an integral part of consumer life” (Muhammad et al., 2018, p. 559). The adoption and use of social media platforms and other channels on the internet means that individuals inevitably leave traces of themselves, which can be used by companies, but also searched by others (Muhammad et al. 2018, p. 559). In the context of the current data, the importance and recognition of a digital footprint became evident. In conducting their own internet searches on the identity of the person a complainant was communicating with, an absence of a social media profiles or a digital footprint became an indicator that the person was not who they portrayed themselves to be. This shows the importance of a digital footprint and how an online presence has now become somewhat of a mandatory requirement for navigating life in the current context (noting that there are some occupations where this is justified and likely required, such as law enforcement or intelligence).

Overall, the use of internet searches to verify or refute any suspicions about the inauthenticity of an identity appears to be an effective mechanism for complainants when implemented. In this way, the current prevention messaging that encourages these types of searches is arguably effective. The challenge remains in the timing of these types of searches. It is clear that not all individuals undertake these searches at the beginning of a relationship or communications. In the current data set, financial loss was recorded by 167 complainants, which affirms that many were suspicious after they had already sent an initial amount of money. Conducting this type of search earlier in the relationship may avoid some of the heavy financial losses and other harms incurred by many victims globally.

Offline Methods of Authentication

While the data clearly indicate a preference to the use of the internet to verify or refute a person’s identity, there was still evidence of actions taken offline to achieve the same outcome. Seeking
assistance from both formal and informal networks was a technique used by a smaller number of complainants. Although the numbers were much smaller, the evidence suggested that in each of these circumstances, the third party was able to establish that the complainant was being deceived. In some ways, this points to the power of third parties to assist with verifying an identity and establishing fraud. However, based on the known victim blaming of fraud victims (Cross, 2015, 2018) and the sense of shame and stigma that they experience, there is a need to overcome the negative stereotype prior to advocating harder for this course of action. It is likely that many of the complainants who undertook their own personal searches did not have the ability to seek assistance from either formal or informal networks.

The results in this section also highlighted the use of private investigators. While the current data set only noted this in two cases, there is a growing private industry that offers individuals access to investigative services (Button, 2019). In the current context, private investigators can be argued to capitalize on the characteristics of online communications, through their offer to verify the person behind an online identity. An Australian example of this can be seen in the company Online Investigations (onlineinvestigations.com.au). This a potential area of growth into the future and worthy of further examination.

The Digital Footprints of Identity Crime Victims

An interesting finding was the use of known fraud and scam websites to alert potential victims to known offenders. The above results point to the effective use of these websites to verify suspicions about inauthentic identities. In conducting an internet search (usually reverse image search), several complainants found that their image was noted on a website indicating that the profile was fraudulent. While this was a positive result for the complainant, and in the cases above, alerted them to the fraudulent nature of the person they were communicating with online, there are perhaps negative, unintended consequences that also need to be considered in this context.

There are a range of websites and forums available, which seek to warn individuals against romance fraud and the use of identities and profiles used by offenders. These can be standalone websites or they can be pages/groups on existing platforms (such as Facebook, Pinterest, or YouTube). The premise behind these sites is to showcase the photos, aliases, false documents, excerpts of communications, and other details that have been used by offenders to target victims to warn others and prevent similar victimization. At its core, these sites are seeking to engage in legitimate prevention activity. This is supported by the results in the current sample, whereby the finding of a photo or details on one of these sites verified the suspicion held by the complainant. However, the above notion of a digital footprint is also relevant to these discussions and the identity crime of these third parties. For individuals whose photos and profiles have been used by offenders, these internet searches directly link their names and identities to romance fraud (among other offenses). The offender has committed identity crime through the misappropriation an innocent person’s photo or details in the first place, and it is arguable that the victimization of this third party is furthered through the linking of their identity to romance fraud. A quick internet search of the term “romance scammer photos” produces multiple pages of images of third parties who have had their photos and identities used by offenders. These individuals now find themselves prominently displayed across a variety of websites, labeled as a fraud. While these websites assert that the person in the photo is an innocent third party, the link to fraud is still clear and explicit. From the perspective of this third party who has had their photo and identity misappropriated by a romance fraud offender, they are a victim of identity crime. There are several high-profile individuals who have been victims to identity crime in the context of romance fraud, and who continue to have their lives impacted upon as a result of the ongoing use of their identities to perpetrate these offenses.
A notable example of this is Bryan Denny. Denny is a retired Lieutenant Colonel from the U.S. Army. Since 2015, when he first received a letter from a romance fraud victim questioning why he didn’t visit her, “he’s identified roughly 4,000 bogus Facebook profiles that utilize a mixture of 51 different photos of him” (Leffler, 2018). His image has been used thousands of times by offenders, under an array of aliases, to defraud victims millions of dollars (Leffler, 2018; Robinson et al., 2019). Denny is contacted on a weekly basis by women from around the world, who believe that they are in a genuine relationship with him, questioning why he hasn’t visited, sent money or made good on promises that “he” made to them. The consequences of this identity crime are enduring and have taken a toll on both him and his family.

There is strong evidence to suggest the impacts of identity crime on victims. Many experience a range of negative effects as a result of having their identities compromised and misused in various ways (Button et al., 2014b; Cross et al., 2016; Lacey & Cuganesan, 2004; Wyre et al., 2020). In particular, victims speak of the struggle to cope with the uncertainty and helplessness associated with not knowing when misuse could happen again (Wyre et al., 2020) and the impact of reputational damage (Button et al., 2014a). Particularly as it related to images, there is emerging research which documents the harms experienced by those who are subject to image-based abuse, where intimate photos are shared publicly (online in many cases) without permission (Powell et al., 2018), as well as those who experience child sexual abuse through the distribution of photos and videos online (Gewirtz-Meydan et al., 2018). While victims may be able to successfully seek the removal of images from platforms, there is a constant fear surrounding the potential for it to resurface along with who will view the image. In a similar vein, those who experience identity crime by romance fraud offenders are constantly waiting for the next notification from a victim. Denny is a prime example of this; despite having successfully removed thousands of Facebook profiles using his photos to attract and defraud women (Robinson et al., 2019), it remains an ongoing struggle.

The linking of genuine identities to fraud may also be problematic in a professional sense. Given the large degree of engagement and use of social media platforms by individuals, employers and recruitment agencies are now using these to vet potential employees (Blount et al., 2016; Delarosa, 2014). Consequently, the negative results from an internet search can become an inhibiting factor that prevents individuals from gaining desired employment. For the case of those who have experienced identity crime and are associated with fraudulent profiles, the permanency of this online record could have ongoing detrimental effects.

In this way, there is a need to think through the ways that successful prevention actions can be taken on the part of potential romance fraud victims to warn against fraudulent profiles, without furthering the damage done to third parties who are victims of identity crime. There is a group of individuals whose digital footprint links them explicitly to romance fraud, despite them taking no part in these activities. Promoting the ongoing use of websites and forums that display photos of fraudulent profiles used by romance fraud offenders is a double-edged sword. While potentially assisting with the prevention of romance fraud, it can further victimize those subjected to identity crime. It also does not prevent offenders from creating new profiles once they have been discovered. Further research and consideration of this context is required into the future to determine an appropriate response, acknowledging the needs of both groups.

**Looking to the Future and the Use of AI**

In response to effective prevention messaging, it is well established that offenders will change their approaches and techniques to effectively target their victims. This is noted by one of the complainants in their observation that “scammers are getting smarter now offering photos that are too far away or side shots making Google image ineffective” (Case 3302). It is also evident in the evolution of approach types as well as communication and payment methods (ACCC, 2020, Cross, 2020a). It
is therefore reasonable to assume that offenders will seek to overcome the perceived effectiveness of complainants using reverse image searching to determine the authenticity of an identity.

Consequently, it is worth considering how AI may be embraced by offenders and seek to overcome the effectiveness of current prevention messaging, and victim-based detection strategies that encourage the use of internet searches (particularly reverse image searches) to verify or refute suspicions of an inauthentic identity. While technology does already exist to manipulate existing images online (such as Photoshop), this does require some level of technological skill and may not bypass the detection methods used by victims. The use of AI-based technology allows for the creation of wholly unique synthetic images that avoid these victim-based detection strategies (Jones, 2020). The use of these synthetic images has already been linked to the creation of fake profiles social media platforms such as Facebook (Gallagher & Calabrese, 2020). Further, there are even dating websites which openly state their use of AI-generated images for their promotional materials (Matthews, 2019).

Currently, existing research is largely focused on the capabilities of AI-generated image or videos, known as “deepfakes” (Westerlund, 2019). These videos have been largely used in the creation of image-based sexual abuse whereby the likeness of individuals is composited onto existing pornography (Westerlund, 2019). Furthermore, the potential of deepfakes in the misrepresentation of public figures has become a focal point in the research as it pertains to political figures and the possible impacts of democratic discourse (Westerlund, 2019). There is less consideration for the potential of offenders using AI-generated images in profiles for fraud. Instead, there has been more of a focus on social bots which essentially spam automatic messages (e.g., political messaging, phishing links).

The use of AI to generate unique images has the potential for offenders to overcome technology designed to catch them (Condliffe, 2020). In the current context, it can potentially reduce the possibilities or effectiveness of conducting reverse image searches on images used by offenders through reducing the possibility for images to be linked to the original source. However, it is worth noting that there would still likely be a need for offenders to create digital footprints of the identity, in addition to the photos, as the above data also demonstrates the suspicion that exists for searches that did not reveal any digital footprint associated with the identity. Should offenders embrace the evolution of AI in their offending behavior, there would need to be a corresponding rethink of prevention messaging to counteract this shift. Further research should consider how the use of AI could be used by all parties to improve responses to inauthentic identities.

**Conclusion**

Romance fraud devastates millions of lives across the globe. Apart from the significant monetary losses that victims incur, there are also substantial nonfinancial harms that negatively impact individuals. Further, given that offenders do not use their own identities to commit fraud, there is an additional group of victims who are subjected to identity crime by offenders misappropriating their photos or other personal information. The subsequent arousal of suspicion on the potential for inauthentic identities is a valid and common circumstance for many who have engaged in online relationships.

This article has examined the ways in which individuals responded to suspicions on the inauthenticity of a person they were communicating with online. Using data obtained from the free text section of romance fraud reports lodged with the ACCC, this article examined the actions that complainants took when confronted with the potential for an inauthentic identity. This analysis indicated that complainants predominantly used an internet search to verify or refute their suspicion, with many choosing to conduct a reverse image search on the profile picture or other photo used by the offender.
The effectiveness of this detection strategy was explored through the yielding of both substantiated and unsubstantiated search results. For those who were able to find the original source of the image used by the offender, the search was able to verify their suspicion and confirm the inauthentic identity of the person they were communicating with online. For those who were unable to find a match for the image, or even find any results relating to the alleged identity, this lack of a digital footprint was sometimes used as evidence to confirm their suspicion of an inauthentic identity. These results show the potential effectiveness of internet searching as a strategy to confirm or deny the legitimacy of a profile or identity used in an online context.

The results also demonstrated the use of fraud websites as evidence to support the inauthenticity of a profile. While this was a positive outcome for the complainant, the linking of third parties, whose identities have been misappropriated by offenders to perpetrate romance fraud, was argued to be somewhat problematic in furthering the impact and potential harm arising from this identity crime. The permanency of a digital footprint that links an innocent third party to fraud and offending behavior through no fault of their own has ongoing implications for the well-being of those individuals.

Overall, these results provide some encouraging outcomes with regard to current prevention messaging. However, it is clear based on current victimization statistics, that not all individuals employ these strategies to confirm an identity as a default action, at the beginning of communications. Rather, the arousal of suspicion about the potential for an inauthentic identity as a catalyst to conduct these searches comes later in the relationship and potentially after the transferal of money. To increase its effectiveness, this needs to be considered in the initial stages of communication and development of an online relationship.

Yet, the promotion of this message is argued to have unintended consequences for those whose identities have been misappropriated by romance fraud offenders. Further, with the evolution of technology and the advancement of AI, it is possible (and likely) that offenders will seek to change their current offending actions to account for this. There is a real possibility of offenders using AI to generate unique images to support their false identities rather than misappropriating others. This would render ineffective a reverse image search, as there would be no original source from which to link the photo.

This article has laid the foundations for future research exploring how to best prevent romance fraud victimization as well as tackle the associated issue of identity crime. The two are inherently linked, and as demonstrated within this article, it is imperative that prevention messaging and the actions encouraged by agencies to potential victims take into consideration how these impact on both groups of individuals. The results of this article point to the need to better understand the actions taken by individuals when confronted with suspicions on the authenticity of the person they are communicating with online. Given the small numbers used for the current analysis, based on the known numbers of romance fraud victims overall, it is worth undertaking research which specifically examines this issue in a more rigorous and systematic way. Second, there is clearly a gap that exists in examining the experiences of those third parties whose identities are misappropriated by offenders to commit romance fraud. The impacts of this type of identity crime and needs of this unique group remain unknown and understudied in current scholarship. Both of these groups present as areas for clear focus and attention into the future, as both romance fraud and identity crime are increasing in their scope and unlikely to disappear from the criminal landscape any time soon.

Authors’ Note

This work has been supported by the Cyber Security Research Centre Limited whose activities are partially funded by the Australian Government’s Cooperative Research Centre’s Program. The authors would also like to thank the Australian Competition and Consumer Commission (ACCC) for their provision of data and their ongoing support of research in this area. The views expressed in this article are those of the authors alone, and
do not necessarily represent those of the Australian Government. All errors and omissions are the sole responsibility of the authors. Gratitude is also extended to Helen Berents, Bridget Harris, Bridget Lewis, and Fiona McDonald for their feedback and suggestions on previous versions of this paper as well as the constructive comments of the three peer reviewers.

Data Availability
The data set used for this article is not available due to restrictions placed on researchers by both the University Human Research Ethics committee and the Australian Competition and Consumer Commission.

Declaration of Conflicting Interests
The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding
The authors disclosed receipt of the following financial support for the research and/or authorship of this article: This study received funding from Cybersecurity Cooperative Research Centre.

Software Information
NVivo version 12 was used in the analysis of this article.

References
Albrecht, C., Albrecht, C., & Tzafrit, S. (2011). How to protect and minimize consumer risk to identity theft. Journal of Financial Crime, 18(4), 405–414.

Allison, S., Schuck, A., & Lersch, K. (2005). Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics. Journal of Criminal Justice, 33(1), 19–29.

Anderson, K. (2006). Who are the victims of identity theft? The effect of demographics. American Marketing Association 25(2), 160–171.

Anonymous. (2019). Follow the footprints. Community Practitioner, February, 14–16.

Australasian Centre for Policing Research. (2006). Standardisation of definitions of identity crime terms: A step towards consistency (Report Series 145.3). http://www.aic.gov.au/crime_types/economic/idfraud.html

Australian Competition and Consumer Commission. (2020). Targeting scams: Report of the ACCC on scams activity 2019. https://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity/targeting-scams-2019-a-review-of-scam-activity-since-2009

Berg, S. (2011). Identity theft causes, correlates and factors: A content analysis. In T. Holt (Ed.), Crime on-line: Correlates, causes and context (pp. 225–248). Carolina Academic Press.

Blount, J., Wright, C., Hall, A., & Bliss, J. (2016). Social media: Creating student awareness of its use in the hiring process. Southern Journal of Business and Ethics, 8, 202–217.

Burns, S., & Roberts, L. (2013). Applying the theory of planned behaviour to predicting online safety behaviour. Crime Prevention and Community Safety, 15(1), 48–64.

Button, M. (2019). Private policing. Routledge.

Button, M., Lewis, C., & Tapley, J. (2009). A better deal for victims: Research into victims’ needs and experiences. National Fraud Authority.

Button, M., Lewis, C., & Tapley, J. (2014a). Not a victimless crime: The impact of fraud on individual victims and their families. Security Journal, 27(1), 36–54.

Button, M., McNaugton Nicolls, C., Kerr, J., & Owen, R. (2014b). Online frauds: Learning from victims why they fall for these scams. Australian and New Zealand Journal of Criminology, 47(3), 391–408.

Chang, J., & Chong, M. (2010). Psychological influences in e-mail fraud. Journal of Financial Crime, 17(3), 337–350.
Chen, C., & Huang, L. (2011). Online deception investigation: Content analysis and cross-cultural comparison. *International Journal of Business and Information, 6*(1), 91–111.

Condliffe, J. (2020). Stopping fake accounts is a cat-and-mouse game. Can Facebook win with AI? *Protocol*. https://www.protocol.com/facebook-machine-learning-fake-accounts

Couch, D., Liamputtong, P., & Pitts, M. (2012). What are the real and perceived risks and dangers of online dating? Perspectives from online daters. *Health, Risk and Society, 14*(7-8), 697–714.

Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology, 21*(2), 187–204.

Cross, C. (2018). Denying victim status to online fraud victims: The challenges of being a “non-ideal victim.” In M. Duggan (Ed.), *Revisiting the ideal victim concept* (pp. 243–262). Policy Press.

Cross, C. (2020a). $2.5 billion lost over a decade: “Nigerian princes” lose their sheen, but scams are on the rise. *The Conversation*. https://theconversation.com/2-5-billion-lost-over-a-decade-nigerian-princes-lose-their-sheen-but-scams-are-on-the-rise-141289

Cross, C. (2020b). Romance fraud. In T. Holt & A. Bossler (Eds.), *Palgrave handbook of international cybercrime and cyberdeviance*. Palgrave.

Cross, C., Dragiewicz, M., & Richards, K. (2018). Understanding romance fraud: Insights from domestic violence research. *British Journal of Criminology, 58*(6), 1303–1322.

Cross, C., & Holt, T. (2021). The use of military profiles and narratives in romance fraud schemes. *Victims and Offenders, 16*(3), 385–406.

Cross, C., & Kelly, M. (2016). The problem of “white noise”: Examining current prevention approaches to online fraud. *Journal of Financial Crime, 23*(4), 806–828.

Cross, C., Richards, K., & Smith, R. (2016). *Improving the response to online fraud victims: An examination of reporting and support*. Australian Institute of Criminology.

Delarosa, J. (2014). From due diligence to discrimination: Employer use of social media vetting in the hiring process and potential liabilities. *Loyola of Los Angeles Entertainment Law Review, 35*(3), 249–280.

Drew, J., & Cross, C. (2013). Fraud and its PREY: Conceptualising social engineering tactics and its impact on financial literacy outcomes. *Journal of Financial Services Marketing, 18*(3), 188–198.

Federal Trade Commission (n.d.). What you need to know about romance scams. https://www.consumer.ftc.gov/articles/what-you-need-know-about-romance-scams

Fletcher, N. (2007). Challenges for regulating financial fraud in cyberspace. *Journal of Financial Crime, 14*(2), 190–207.

Gallagher, F., & Calabrese, E. (2020). Facebook’s latest takedown has a twist—AI-generated profile pictures. *ABC News*. https://abcnews.go.com/US/facebooks-latest-takedown-twist-ai-generated-profile-pictures/story?id=67925292

Gewirtz-Meydan, A., Walsh, W., Wolak, J., & Finkelhor, D. (2018). The complex experience of child pornography survivors. *Child Abuse and Neglect, 80*, 238–248.

Holt, T., & Turner, M. (2012). Examining risks and protective factors of on-line identity theft. *Deviant Behavior, 33*(4), 308–323.

Internet Crime Complaint Centre. (2020). 2019 Internet crime report. https://pdf.ic3.gov/2019_IC3Report.pdf

Jiang, L., Bazarova, N., & Hancock, J. (2011). The disclosure—Intimacy link in computer-mediated communication: An attributional extension of the hyperpersonal model. *Human Communication Research, 37*(1), 58–77.

Jones, V. (2020). *Artificial intelligence enabled deepfake technology: The emergence of a new threat*. ProQuest Dissertations Publishing.

Jorna, P., Smith, R. G., & Normal, K. (2020). *Identity crime and misuse in Australia: Results of the 2018 online survey*. Australian Institute of Criminology.

Lacey, D., & Cuganesan, S. (2004). The role of organizations in identity theft response: The organization–individual victim dynamic. *Journal of Consumer Affairs, 38*(2), 244–261.
Leffler, D. (2018). This army veteran became the face of military romance scams. Now he’s fighting back. Task 
& Purpose. https://taskandpurpose.com/news/military-romance-scams-bryan-denny

Lynch, J. (2005). Identity theft in cyberspace: Crime control methods and their effectiveness in combating 
phishing attacks. Berkeley Technology Law Review, 20, 259–300.

Matthews, H. (2019). Generated photos allow dating sites to use photos of AI-rendered faces to make their 
platforms more welcoming to users. https://www.datingadvice.com/online-dating/generated-photos-can-
makeldating-sites-more-welcoming

Milne, G. (2003). How well do consumers protect themselves from identity theft? The Journal of Consumer 
Affairs, 37(2), 388–402.

MTV (2020). Catfish: The TV show. http://www.mtv.com.au/catfish-the-tv-show

Muhammad, S. S., Dey, B. L., & Weerakkody, V. (2018). Analysis of factors that influence customers’ will-
ingness to leave big data digital footprints on social media: A systematic review of literature. Information 
Systems Frontiers, 20, 559–576.

Netsafe (n.d.). Romance scams. https://www.netsafe.org.nz/romance-scams/

Nhan, J., Kinkade, P., & Burns, R. (2009). Finding a pot of gold at the end of an internet rainbow: Further 
examination of fraudulent email solicitation. International Journal of Cyber Criminology, 3(1), 452–475.

Peakey, K. (2019). Women “victims in 63% of romance scams.” BBC News. https://www.bbc.com/news/
business-47176539

Piquero, N., Cohen, M., & Piquero, A. (2011). How much is the public willing to pay to be protected from 
identity theft? Justice Quarterly, 28(3), 437–459.

Pontell, H. (2002). “Pleased to meet you . . . won’t you guess my name?” Identity fraud, cyber-crime, and white-
collar delinquency. Adelaide Law Review, 23, 305–328.

Powell, A., Henry, N., & Flynn, A. (2018). Image-based sexual abuse. In W. DeKeseredy & M. Dragiewicz 
(Eds.), Routledge handbook of critical criminology (2nd ed., pp.305–315). Routledge.

Robinson, L., Rubinsztein-Dunlop, S., Anderson, B., & Dredge, S. (2019). Bryan Denny is the face of military 
romance scams, and he wants it to stop. ABC News. https://www.abc.net.au/news/2019-02-12/facebook-
bryan-denny-is-the-face-of-military-romance-scams/10786180

Scamwatch (n.d.). Dating and romance. https://www.scamwatch.gov.au/types-of-scams/dating-romance

Schlosser, A. (2020). Self-disclosure versus self-presentation on social media. Current opinion in Psychology, 
31, 1–6.

Seda, L. (2014). Identity theft and university students: Do they know, do they care? Journal of Financial Crime, 
21(4), 461–483.

Smith, R. (2011). International identity crime. In C. Smith, S. Zhang, & R. Barberet (Eds.), Routledge handbook 
of international criminology. (pp. 142–152). Routledge.

Steel, A. (2010). The true identity of Australian identity theft offences: A measured response or an unjustified 
status offence? University of New South Wales Law Journal Forum, 16, 1, 48–55.

Vieraitis, L., Copes, H., Powell, Z., & Pike, A. (2015). A little information goes a long way: Expertise and 
identity theft. Aggression and Violent Behaviour, 20, 10–18.

Wall, D. (2013). Policing identity crimes. Policing and Society, 23(4), 437–460.

Walther, J. (1996). Computer-mediated communication: Impersonal, interpersonal and hyperpersonal interac-
tion. Communication Research, 23(1), 3–43.

Walther, J., van der Heide, B., Ramirez, A., Burgoon, J., & Peña, J. (2015). Interpersonal and hyperpersonal 
dimensions of computer-mediated communication. In S. Sundar (Ed.), The handbook of psychology of 
communication technology (pp. 3–22). John Wiley & Sons.

Westerlund, M. (2019). The emergence of deepfake technology: A review. Technology Innovation Management 
Review, 9(11), 39–52.

Whitty, M. (2013). The scammers persuasive techniques model: Development of a stage model to explain the 
online dating romance scam. The British Journal of Criminology, 53(4), 665–684.
Whitty, M., & Buchanan, T. (2012). The psychology of the online dating romance scam. https://www.scribd.com/document/296206044/The-Psychology-of-the-Online-Dating-Romance-Scam-copypasteeds-com

Wyre, M., Lacey, D., & Allan, K. (2020). The identity theft response system. *Trends and Issues in Crime and Criminal Justice, 592*, 1–18.

**Author Biographies**

**Cassandra Cross** is a Senior Research Fellow at the Cybersecurity Cooperative Research Centre. She is also an Associate Professor in the School of Justice, Queensland University of Technology. Her research focuses on the policing, prevention, and support of fraud victims globally. She is coauthor of the book *Cyber Frauds, Scams and Their Victims* published by Routledge in 2017.

**Rebecca Layt** is a PhD candidate and sessional academic in the School of Justice, Queensland University of Technology. She holds a Bachelor of Justice (Honours) (First Class Honours), a Bachelor of Behavioral Science (Psychology) and a Bachelor of Justice.