GlobalDating Insights .com

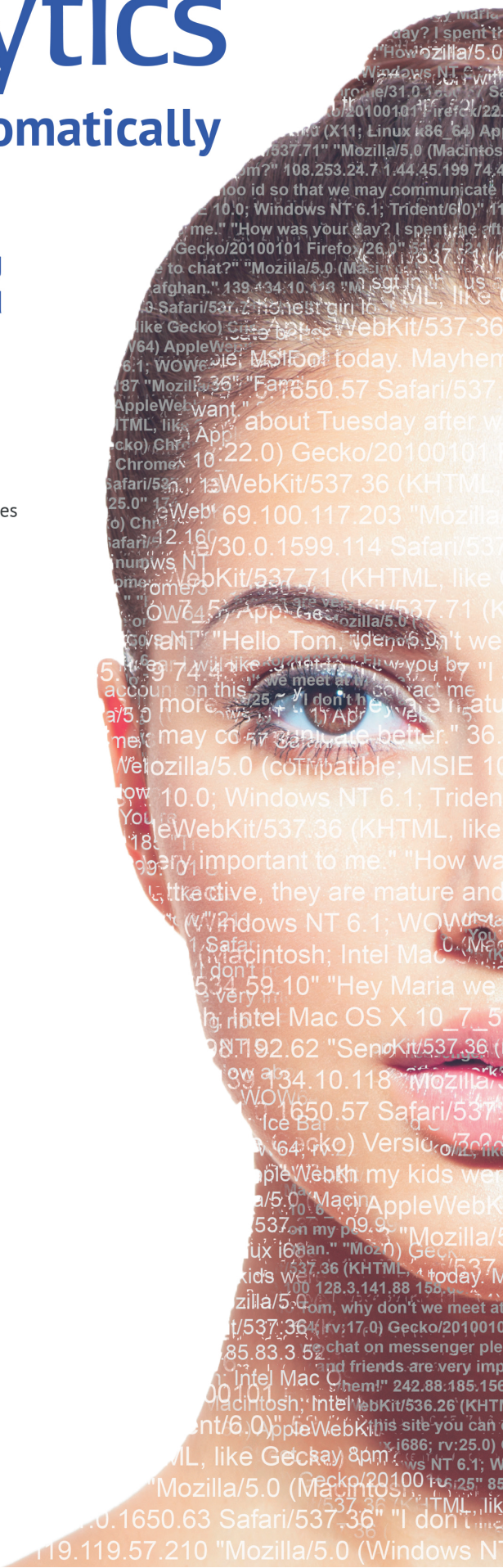
SCAMMERS & ONLINE DATING FRAUD

2015 TRENDS AND TACTICS

SPONSORED BY

Scamalytics

Stop Scammers Automatically



"Scamalytics works like anti-virus for our dating sites. Constantly working in the background and removing scammers and fake profiles saving us time and costs in moderating."

Tanya Fathers, CEO Datingfactory

Scamalytics works with some of the largest dating and social networking sites to stop dating fraud automatically, accurately and quickly.

Our systems combine behavioral analysis, network intelligence, user data analysis, realtime pattern matching and image recognition to catch scammers earlier so reducing the costs of dating fraud.

Clients also tap into the largest shared database of dating scammers allowing them to share early intelligence of text, images and networks that are being used by fraudsters.

Contact us at info@scamalytics.com for a FREE 60 Day Trial

Featured Clients

global personals

Datingfactory private label solutions

TOGETHER NETWORKS

FreeDating.co.uk

LOVESTRUCK

meetville

CupidMedia™

INTRODUCTION/CONTENTS

All consumer businesses have a duty to protect their customers, but for an industry as personal as online dating, it is of utmost importance.

Scammers and online frauds present one of the biggest threats to the safety and privacy of online dating consumers.

There are countless stories of the irrevocable damage done to people's lives at the hands of these criminals, who lurk on dating sites, preying on unsuspecting singles.

And not only are these frauds incredibly damaging to the victims, they are also extremely harmful to the reputation of the industry as a whole, and therefore bad for business.

Taking steps to improve the defenses of online dating services, and keeping up to date with the latest scams, is a must for every company that wants to improve the industry.

In this report, and in collaboration with Scamalytics, we will cover the issue of scammers and dating fraud, looking at the latest trends, the various types of fraud, the latest anti-scammer technology, and the cost of scammers to your business.

While the report is aimed at dating operators, and seeks to offer an in-depth analysis into the topic, for those who want a quick start guide to the problem of scammers, please turn to page 10.

We have also talked to some of the leading sites in the industry, to ask what they are doing to fight scammers, and the regulatory and consumer bodies who have pledged to do their part to educate consumers and enforce good practice amongst the industry.

We hope you enjoy the report!

Simon Edmunds
Editor

TRENDS: TINDER, BOTS AND SEXTORTION

As dating sites and singles have migrated to mobile over the past few years, so too have the dating scammers and fraudsters who leech off the industry.

With the proliferation of apps like Tinder, a whole new pool of potential victims have surfaced, and these sophisticated criminals have acclimatized to this new dating landscape, and adapted their methods in an attempt to entrap these singles.

And just as dating sites cater to different niches, scammers also tailor their frauds, depending on the clientele of the service.

Rather than the "romance scam" fraud seen on many dating websites, scammers on mobile apps are instead using advanced lovebots to lure in their victims, or by posing as prostitutes.

Last July, security experts Symantec released a report that said apps like Tinder had three main types of spam bots infecting their service.

These were adult webcam spammers, lovebots and fake prostitution profiles.

The first type would tempt users to click a link to another site. And as with all scammer campaigns, they evolved - modifying their scripts, switching to short URLs like bit.ly, and eventually asking users to move the conversation to Kik messenger to "close the deal".

The second type were those promoting a third party - such as bots pushing mobile games like Castle Clash, which last April invaded Tinder, creating a lot of negative media attention for the company.

After users matched with the bots, the "women" would strike up a conversation, quickly ask whether their match had heard of a game, and send them a link - in the case of the Castle Clash bots, containing the URL "Tinderverified".

These disappeared, but the same script can be, and was, adapted for different games, webcams and services.

The bots, which often use phrases like "looking for someone to curl up watch a movie with or football or just hang out", or "a little facial hair is a plus and someone with an awesome personality is key", can also be highly sophisticated.

Dan Winchester, co-founder of Scamalytics, said:

"We see whole conversations unfold between humans and bots, with the human believing they are talking to another human - effectively passing the Turing test! The bot will ultimately move the human onto another messaging platform or service, or alternatively harvest an email address."

The other type of spam, which Symantec said makes up the "overwhelming majority" of spam on mobile, are fake prostitution profiles.

tinder™

These have provocative pictures of women, with a text overlay giving details about price and services, and a URL to connect with the women. These URLs take you to explicit personals websites for casual dating and hookups.

Symantec said what these campaigns all have in common is affiliate programs, which pay scammers if the campaigns are successful and leads are converted.

One such affiliate program, for blamcams, ran a three month campaign with seven different URLs, that resulted in half a million clicks. Such programs might pay $6.00 per lead for a successful sign-up, and $60 if a lead becomes a premium member, Symantec's Satnam Narang said.

Security experts have also noticed that as scammers follow the flock of millions dating on mobile, they also learn to change their tactics quickly, when new security measures are introduced.

Following Symantec's report, Tinder released an update, designed to cut out these types of fraudulent profiles, which their director of comms, Rosette Pambakian, said was "a major technical solution to our current spam issue."

However since then another report, by Pindrop Security, showed how scammers had swiftly adapted their tactics to combat the introduction of these measures.

They found that a whole new type of complaint was being reported, with fraudsters asking for a user's phone number, and continuing their spamming tactic via SMS.

Pindrop's Raj Bandyopadhyay and Valerie Bradford said:

"When the security of the online channel is improved, fraudsters switch to the phone channel, which has historically been under-protected. This lack of security innovation on the phone channel makes the phone a preferred vector for financial attacks.

"The Tinder phone spam complaints are yet another example of the connection between cybercrime and phone fraud. Fraudsters today adapt quickly to changing technology and security measures, and are very capable of launching a multi-pronged spam attack – much like their cybercriminal counterparts."

Another new form of scam that has been rising over the past few years is "sextortion".

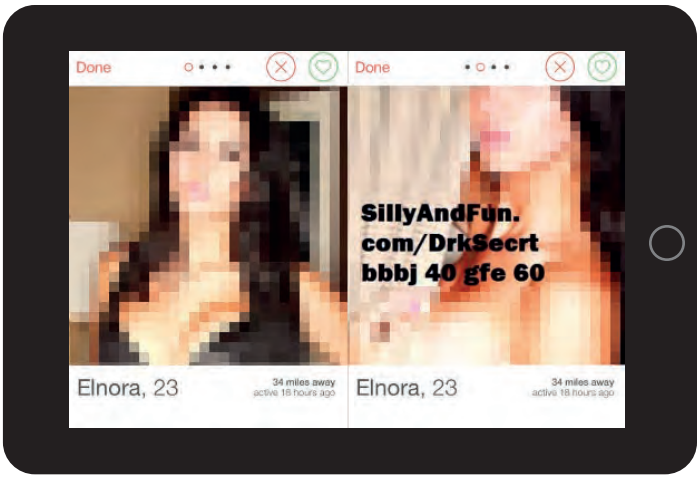
This is where people are lured into a webcam session with who they think is an attractive woman, after accepting a friend invitation on a social media or dating site.

As they video chat to this woman - who is often a pre-recorded video whose actions can be controlled by the fraudster - their webcam is recorded.

Victims are subsequently blackmailed, the scammer saying they will post the video online, or send it to their loved ones, unless they transfer huge amounts of money into an offshore bank account.

There have been thousands of victims of this increasingly common scam, with fraudsters often targeting teens, who are more susceptible to this particular type of fraud.

Anti-scammer group Scam Survivors said sextortion will be one of the biggest trends to watch in 2015, and while it will generally affect adult and casual dating services, general dating sites need to be mindful.



According to Scam Survivors, customers of some of the largest social and dating websites - including Facebook, OkCupid, POF, Kik, Skout, Tagged, Tinder and more - have reported sextortion scams to them in 2014.

And stories of these types of fraud have also been rife in the media - further alerting potential customers to the industry's problems - whether it be the cleavage selfies of Karen Danczuk being used for fake profiles, or gangs of scammers being locked up for their crimes.

While many think of dating fraud as the oft-written about romance scams, there are many other sophisticated ways that fraudsters are infecting mobile and desktop sites, in an attempt to ensnare singles.

Keeping abreast of such developments, and the adapting nature of such scams is a constant battle, but one our industry must fight head on if we want to move forward, and increase trust in online dating.

WHAT ARE YOUR DATING COMPETITORS DOING, AND WHY?

Online dating is an incredibly competitive industry, with companies constantly looking for ways to get a foothold over competing sites, as they vie for the attention of singles.

And while sites want to offer a better service for their customers, these digital businesses are also obviously striving to simultaneously increase their revenue.

By taking steps to stop scammers, dating businesses are able to achieve both, and the benefits work together - as customers stay on the service for longer, reputation stays high, and the business avoids churn, poor LTV and chargebacks.

We asked some top sites in the industry about the steps they take to suppress scammers on their sites, and how the implementation of such measures has affected the performance of their business:

Laurence Holloway
Co-founder and CTO
Lovestruck:

"Apart from the obvious risk of some members being defrauded and put in serious danger, allowing any scammers onto the service would be deeply damaging to the inherent level of trust in a dating service for everyone. If a scammer is able to send messages to genuine members, even for only a brief time, the reputation of the service is compromised.

We are highly active in the detection and removal of any accounts that breach our terms of use. This obviously includes scammers and fraudsters who routinely target all dating services. We have our own systems that constantly analyze both the content and behavioral patterns of messaging and profiles, plus we are trialing the use of Scamalytics inside our main moderation system, to provide a deeper level of protection against scammers who are trying to mask their location and identity.

This all works in symphony to prevent scammers getting their accounts approved, and being able to contact our members.

We also "auto-ban" accounts whose messaging behavior is suspicious.

All fake accounts are removed at source, so this increases our rejection rate and load on our moderation services. Our LTV is not affected, however."

Ross Williams
Founder and CEO of
White Label Dating:

"Protecting consumers from fraud should be the utmost priority for any ecommerce business, and online dating is no different. As an industry, we have a duty of care to help our members find love in the safest possible environment. Scammers prevent that from happening. That's why our fight against scammers is so important.

At White Label Dating, we take a number of steps to prevent scammers from coming into contact with our members. Our in-house 30-strong team of highly trained moderators work 24 hours a day, 7 days a week, 365 days a year, to monitor every item of user-generated content submitted, including all photos, profile text and first message. First messages account for around 20% of moderated items. The team work in tandem with Scamalytics to predict scammer behavior and quickly remove scammers from our platform.

The majority of scammers are removed from our platform within seconds of joining, before they have the opportunity to interact with our members. That means that they don't really affect churn or LTV.

Scammers are often easily identifiable through the language that they use. When creating a profile, they may use tried and tested text that doesn't reveal their true identity. However, when writing a message, they're easily caught out. Of all the scammers we identify, we catch more than half through first message moderation. They're then instantly removed and never have the chance to come into contact with members."

Tanya Fathers
Co-founder and CEO of Dating Factory:

"Scammers create bad user experience on the sites, but also create fraudulent payment transactions that normally result in chargebacks. So stopping the scammers gives benefits to both users and merchants at the same time. We use an in-house team to manually check and approve/delete profiles of all new users based on the risk score – which is a combination of our internal knowledge and the Scamalytics score.

Regarding churn, it is not affected, as we catch them before that. We have the system in place from day one, so we cannot compare to any previous experience of "not fighting scammers"."

Jennifer Doherty
Fraud Prevention Associate at CupidMedia:

"People come to our sites to meet their perfect match, and they expect a safe environment with genuine contacts. It's important our customers have a safe, enjoyable and rewarding experience, and scammers of course detract from that. It's not just a matter of a customer losing money: once someone realizes they're in contact with a scammer, their trust has been violated – in the person they were in contact with, in our website, and in the online dating industry as a whole.

CupidMedia's dedicated Fraud Prevention Team uses an extensive suite of in-house and third party technologies to rapidly catch scammers. We also feel that user education is important, and display safety tips at key points on our site, such as the mail system, while also maintaining an extensive web guide to safe online dating.

Encountering scammers will inevitably lead to a bad customer experience, and a bad customer experience will naturally increase churn."

SCAMMIEST COUNTRIES

IP addresses can tell you the location of the user, and what ISP they are using. But in this world of proxies and TOR networks, this information can often be disguised.

According to the latest Scamalytics data, scammers that targeted the US (ranked by total number) originated from:

1. **United States**
2. **Philippines**
3. **United Kingdom**
4. **Anonymous Proxy**
5. **Nigeria**
6. **Ghana**
7. **Canada**
8. **Australia**
9. **Netherlands**
10. **South Africa**

419 Scams

This is the classic "romance scam", where the user is enticed by false hopes of romance to send money abroad.

The classic romance scammer befriends a victim online and sweet-talks them into a strong, personal long-distance relationship. The scammer then undergoes one major crisis after another (with complications), meaning that they defraud the mark not just once, but time-and-time again.

The Australian Competition and Consumer Commission (ACCC) in Australia has recently taken direct action to warn Australian citizens they think might be at risk of this scam - by identifying the riskiest targets based on overseas bank transfer records.

In the documentary "419: The Internet Romance Scam", Barney Lankester-Owen explains:

"Not only is internet fraud growing but it's evolving. These con artists are experts at psychological manipulation and will do anything to get money off their targets, even meeting up in person and having offline relationships to secure a steady stream of money."

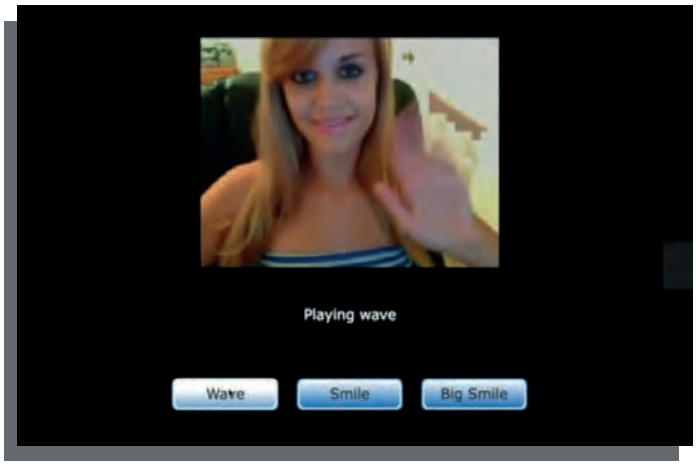
Business threat: Whilst not many people fall for these scams, plenty experience them in the form of improbable profiles and dubious approaches. The result is early churn from users who might otherwise convert or maintain a longer subscription, not to mention a reputational threat when the media spots obvious fakes on a dating site.

Cam-Girl Fraud

Some women with a webcam exhibit for money, using either their own website, or one of the aggregation platforms for cam-girls.

This scam aims to get the target to go directly to the woman's own webcam, where they can be charged. Also see redirection.

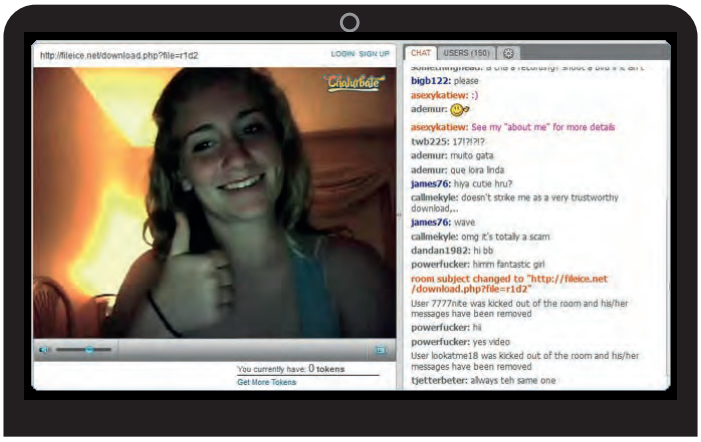
Business threat: Worst case scenario is the dating site loses the user to the cam site. However, the remaining users can be left wondering if there are any genuine women on the dating site - and either don't convert, or churn early.



Sextortion

A relatively new type of fraud, becoming increasingly well organized. The scammer engages in chat with the target, which becomes sexual and moves off the dating site. The target is enticed into producing some sort of blackmailable material, such as engaging in sexual behavior on webcam. The material is then used to blackmail the target.

Business threat: Users experience fake profiles, deceptive conversations, and lose faith in the dating site and its member base. This leads to lower conversions and high churn rate.



Virtual Cam Whores (VCWs)

This is a variation on the cam-girl fraud, but requires no real models in front of the camera, as they are virtual recorded videos, manipulated by the operator. The scammer basically has control of a virtual video and, like a marionette puppet, can issue commands such as "wave" or "wink" etc.

Business threat: Similar to that of cam-girl fraud and the sextortion scams, which are using VCWs.

Redirection Fraud

Affiliates (or even unscrupulous dating site operators) attempt to move the target off the host dating site, and onto a new dating site.

For example, the fraudulent profile might claim to have a paid account on the alternative site, and suggest chatting there instead of on the host site. Some cam-girl fraud is actually redirection fraud.

Business threat: Potential to lose users to a competitor; bad experience for everyone else.

Affiliate Fraud

In this case, the dating site is being defrauded by their own affiliates. The affiliates might create fake profiles, or entice real people to sign up with a fake deal (for example free iPad on joining), take the payments and then disappear before the fraud is uncovered.

Business threat: Affiliate budget is wasted on worthless profiles; bad experience for the genuine users.

Credit card Fraud

Organized scammers use stolen cards to gain full access to the target dating site.

Scammers will also test stolen cards on sites with no product to physically fulfil, making dating sites an ideal target.

Business threat: Higher banking fees and chargebacks.

Top University Networks Used by Scammers

According to Scamalytics, some scammers are hacking or gaining access to university networks. Here are the top 10 university networks most popular with scammers (January 2015 figures):

1. **Boston University**
2. **Utah State University**
3. **Rutgers University**
4. **University of Waterloo**
5. **UniNet (Inter-university network)**
6. **University Corporation for Atmospheric Research**
7. **University of Michigan**
8. **University of Minnesota**
9. **City University**
10. **SungKyunKwan University**

THIRD PARTIES

The scammer ecosystem extends beyond just dating sites - the typical scammer will also require a separate communication platform upon which to execute the scam, and a way for the target to transfer money.

The third party communication platform might be instant messaging (such as Yahoo Messenger), email, a social networking site such as Facebook, VOIP (typically Skype) or regular telephony.

Names of third party messaging systems which appear undisguised in scammer messages

Yahoo	12.6%
Gmail	5.0%
WhatsApp	3.8%
Facebook	3.3%
Skype	2.7%

Source: *FreeDating.co.uk, Q4 2014.*

Dan Winchester, co-founder of Scamalytics, said:

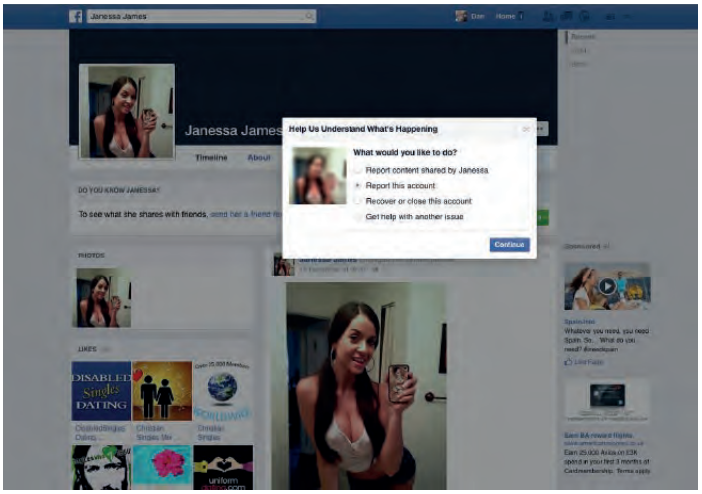
"While Yahoo still appears to be the platform of choice for dating scammers, other platforms are gaining in popularity, due to particular benefits they confer in executing the scam.

"WhatsApp permits geographic phone numbers, giving the scammer the ability to "place" themselves in the same country as the target, whether or not this is actually the case.

"Facebook allows the scammer to create a credible fake identity. Sometimes we will see scammers with hundreds of friends, who actively contribute to that scammer's timeline. On closer inspection, the "friends" are mainly fakes too."

Once the target is primed, the scammer needs a way for the victim to transfer money. This might be an overseas money transfer service, such as Western Union or MoneyGram. The ACCC actively monitors large transfers through services such as Western Union to high-risk regions like West Africa. They contact the transferor, alert them to the likelihood that they are being scammed, and urge them to stop sending money.

According to victim support forum Scam Survivors, other payment methods that scammer use include Amazon Gift Cards, which are impossible to be cancelled, and PayPal, which is very expensive to cancel.



And the new wave of organized sextortion scams have even led to reports of some scammers accepting credit cards - and because the target is already being blackmailed, they are highly unlikely to charge back.

BUY OR BUILD

"Effective scammer protection" is not a USP you often see in dating site marketing campaigns. This backend problem tends to come under the category of "firefighting" rather than "features", so is it a good candidate for outsourcing, in the same way that managed hosting or anti-virus is?

One of the main advantages of outsourcing is, of course, cost control. Scamalytics charge a flat rate per user, meaning that you pay a fixed rate each month, regardless of whether or not you get hit by unexpected scams.
Co-founder Nick Tsinonis said:

"Part of what we are selling is a predictable monthly cost for an effective solution - we build in burstable margins, so if a client is hit by a large and unexpected attack, they won't pay more for that".

Many dating sites still like to retain an element of protection in-house though, for example Lovestruck, a high-end dating site based in the UK that caters to busy professionals.
Laurence Holloway, the co-founder and CTO said:

"We take a hybrid approach: some elements are better if engineered in-house and deeply embedded in the heart of your own systems, but specialist information (and external, shared knowledge) will always be more powerful in certain areas of fraud detection, due to a much larger data set and collaborative algorithms."

This highlights a second advantage of outsourcing: sharing intelligence and techniques across the wider industry. Most of the third party systems, such as Maxmind, Iovation, Threatmetrix and Scamalytics, have data-sharing at the core of their products. In the case of Maxmind, that might be a high-risk IP address. Iovation and Threatmetrix both look at risky devices. Scamalytics take profile data and message text, and compare it to known scammers and bots.

Some dating sites take a "belt and braces" approach, by combining multiple third-party solutions, along with their own internal systems.

Jennifer Doherty, from Cupid Media's Fraud Prevention Team, said:

"It's important to create a multi-pronged and multi-layered defense against scammers, to catch them at all potential touch points. A combination of technology purchased from third parties, and internally-built detection around your specific requirements, is the strongest defense against scammers."

White Label Dating also take the hybrid approach, but with an emphasis on developing in-house moderation expertise, as co-founder and CEO Ross Williams explains:

"A combination of buying and building scammer detection is what we've found to be the most effective way of combatting scammers. Technology like Scamalytics is great for determining scammer trends and removing scammers displaying obvious behavioral patterns, but human identification will always be essential. With scammer techniques becoming more advanced, it takes a human eye, knowledge and instinct to stop the most advanced scammers in their tracks."

A third benefit of outsourcing is to free up value dev resource, to focus on product differentiators, such a new features, growth hacking, or supporting new devices. Fighting scammers is a massive duplication of effort across the industry, which is more efficiently managed by a centralized team. Your software development team is your most highly-prized and over-utilized asset. You should be dedicating every hour of development time on improving your product and growing your market share, not reinventing the wheel each time a new scam or fraud technique comes along.

By Dan Winchester, co-founder of Scamalytics

QUICK START: AN INTRODUCTION TO THE SCAMMER PROBLEM

Any platform that allows communication between two or more strangers is open to exploitation by scammers.

Online dating is particularly attractive to scammers as users are receptive to contact from broadly unqualified strangers, which enables the scammer to easily create a false identity.

There are a variety of common scams (see "Types of Fraud"). Some of these target the user in an attempt to get money out of them directly, and some defraud the host dating site, for example by moving genuine users onto a competing site, or defrauding the site's affiliate scheme.

All scammers, be they human or bots, need two minimum requirements in order to execute a scam:

- **The scammer needs to create a false identity.** These are almost always in a different geographical location to their true identity, with false photos, profile text, age, and even gender. Not only does this protect their identity, but it establishes credibility and/or desirability.

- **The scammer will attempt to move the target off the host messaging system.** The moment the scammer is detected by the dating site, their communication channel with the target is cut off, so they need to move the target onto a less secure messaging system as early as possible. In some scams, the sole objective is to move the user onto another dating site.

Attempts to detect scammers typically look at the characteristics which follow from these two requirements - for example using a fake photo, accessing the site from a country other than their stated location, or sending contact details in messages.

Examples of some basic tests include:

- **Checking the user's IP, using an IP lookup service such as Maxmind, and ensuring it matches their stated location.**

- **Checking the user's photo, using Google image search.**

- **Scanning messages for scammy phrases such as "god fearing".**

As well as removing scammers, education has an important part to play in tackling the problem. The issue has attracted plenty of mainstream media coverage, largely focusing on the financial and emotional cost to victims.

Australian consumer watchdog, the ACCC, advises dating sites to inform users about risk from scammers as part of their Best Practice Guidelines. In the UK, the Online Dating Association requires that member sites have "easily accessible safety information for users, explaining the potential risks with online dating", and ensure that "all user profiles are checked and that appropriate arrangements exist to detect fraudulent or misleading profiles".

Research from Scamalytics suggests that a typical mainstream site can expect between 5% and 10% of new profiles to be fraudulent.

All these fake profiles need to be detected and removed before they can interact with genuine users.

And while techniques to detect these fake profiles can be implemented, scammers constantly find new strategies to circumvent them, making the fight against scammers an on-going battle.

Regulatory Authorities

As dating sites work to combat the threat of scammers, there are also a number of consumer and regulatory bodies who are seeking to influence the issue, through both education and enforcement. Such organizations can help by promoting good practice in the industry, while also educating consumers, help them report dating fraud, and intervene in criminal activity. Here are some bodies who have committed to help stamp out dating fraud:

Australian Competition and Consumer Commission (ACCC)

This Australian organization has been very proactive in the online dating sector.

Last year, they launched their Scam Disruption Project, which utilized financial intelligence to "identify Australians who were sending funds to West African nations". The ACCC then got in contact with these people, to say they may have been targeted by a scam.

The ACCC also conducted a sweep of dating sites, looking for "misleading offers, unclear pricing policies or consumer contracts with unfair terms", along with what measures dating sites had in place to protect consumers against scammers - the results of which are due in a month or two.

Sites that signed up to the ACCC's Best Practice Guidelines said they were initially concerned that sending scam warning messages might discourage customers. However feedback from those who adopted the recommended measures "indicates that customers have responded positively and felt secure in the knowledge that service providers were actively protecting their interests."

The Online Dating Association (ODA)

The ODA is a UK-based regulatory body that counts Match.com, eHarmony, Lovestruck and Oasis amongst their members.

The Chief Executive of the ODA, George Kidd, said that "protecting our users from harm, deception and loss" was one of their key principles when the body was set up.

ODA members - who must sign up and adhere to a code of practice - commit to "checking profiles, giving advice and guidance to customers, and dealing promptly with reports of fraud or other problems", while also offering inservice mail and chat forums, and talking to police about reducing scams.

Their Date Safe campaign worked with Action Fraud, the Metropolitan Police and other UK organizations, to educate the public on dating scams. They have also held scammer workshops to let sites share best practice for combatting scammers, and plan future events in collaboration with leading police agencies.

Action Fraud and Operation Falcon

The UK also has Action Fraud, a national organization that lets consumers or companies report fraud, or attempted scams and viruses. Dating sites can also use their business reporting tool to report scammers in bulk.

Last year, they alerted online dating customers about the growing types of dating fraud that had been reported to them.

In October 2014, the Metropolitan Police launched operation Falcon, designed to crack down on online dating scammers. Although the campaign is part of a larger war on cybercrime and fraud, online dating fraud was recognized as a growing area of concern.

Federal Trade Commission (FTC)

The FTC's client is the US government, and therefore the public. They seek to educate consumers, propose legislation, enact rules and take law enforcement action. Although a civil agency, their enforcement tools include civil penalties (fines), the power to go directly to federal court to freeze corporate and personal assets, obtain injunctions, and return money to victims.

In serious cases they can hand over information to relevant law enforcement agencies, and encourage criminal authorities to take action.

They told us they do "not bring cases on behalf of individual consumers", but rather by looking for a "pattern of deceptive conduct" which "often comes from receiving consumer complaints, but not always".

For the first time last year, the FTC charged a dating site, British-based JDI Dating, for allegedly using fake profiles to lure customers into subscriptions, ordering the company to pay $616,165.

CONSUMER ACTION GROUPS

Victims and consumers are turning to online self-help groups to help victims recover from the psychological and financial effects of falling prey to scammers. One of them, well-known in the dating industry, is Scam Survivors.

As their website says: "Scammers will take your money with no cares about what its loss means to you or how it affects you. You are nothing but a money amount to them - a living, breathing ATM machine. This is why our site exists." Scam Survivors and similar consumer action groups have one or more of the following goals:

- To make the lives of scammers more difficult, by exposing their photos, emails and attachments to search engines.

- Educating the public. Letting internet users understand that dating can be fun and rewarding, but they need to learn about the signs of the obvious, and the not-so-obvious, tricks that scammers use to suck in a victim.

- Helping victims of scams accept that they can move forward and recover from the psychological and financial effects caused by scammers.

Wayne May, the CEO of Scam Survivors, who has single-handedly exposed a number of scammers, spoke about the state of scamming in the dating industry, saying:

"Stopping all scammers is impossible. The key thing now is education. The more people are aware of the scammers and how they work, the harder it'll be for them to find victims."

In January 2015, it was reported that Jan Marshall from Melbourne, Australia who lost AUD$250,000 to a scammer has also set up a group for victims of similar crimes on Meetup. The ACCC said that Australians probably lost an estimated AUD$90m in 2014.

According to an article in the Canberra Times in Dec 2014:

"There are 1000s of scambusting sites, including Pigbusters, Stolen Valor, Military Imposters Awareness, 419Eater.com, ScammingScammers, Women Who Hate Nigerian Romance Scammers, and RomanceScam.com. Others, like the man calling himself Nigerian Scamhunter, post YouTube videos and warnings, showing potential victims how to see if an image has been stolen by a romance scammer. Scamming the scammers makes good radio for New Jersey scam hunter and comedian Davin Rosenblatt. To fool scammers, the cast of his radio show Davin's Den concoct characters and stories as crazy and convoluted as those devised by the bad guys to suck in victims. A character, Joe Currie, told a female scammer he could only pay in drachmas and yaks."

Organizations and groups like these are normally run by volunteers who are passionate about educating consumers and supporting victims, but they are also very active in helping authorities find and catch scammers around the world.

Today's scammers are not just lone cowboys sitting at internet cafes in West Africa manually typing out messages, but more likely to be sophisticated dark web "businesses" and highly technical cybercriminals looking to make millions from unsuspecting victims.

Scammers are either trying to take money from the dating site itself, or make money from dating customers who get tricked into handing money over for a personal crisis, investment, fake charity or any one of hundreds of "sounds-too-good-to-be-true" business opportunities.

Scamalytics research has shown that scammers from different countries use different methods and that cultural beliefs may even play a strong part in justifying, or even supporting their intentions.

Nigeria - Uzodinma Okpechi - I Go Chop Your Dollar - YouTube[sub].avi With subtitle

West African Scammers - Nigeria and Ghana (Ogas and Sakawas)

Some West African scammer gangs justify scams by saying they have a claim to money which was stolen from them in the slave trade or during British and American colonialism.

There are even pop songs written about this, such as the Nigerian song "I Go Chop Your Dollar", where 419 scams are glamorized with lyrics like: "I go take your money and disappear. 419 is just a game. You are the loser. I am the winner".

According to Scam Survivors, these scammers can work alone, but the richest, most powerful Nigerian 419 scammers get others to do the groundwork for them.

Like the internet marketing conversion funnels, they use teams of five or more to help them get through the thousands of users needed to achieve a successful hit rate. The first level is to mass email dating site users, then the marks are identified and pushed through to an expert, who chats to them, and converts the marks into "customers".

Each person in the chain gets paid for their role in the lead generation, but the person making the most money and executing the sophisticated and manipulative scams is the Oga (or boss) who then owns the "customer". Alongside romance scams, they also execute other 419 scams that have been widely covered in the media over the past few years. South Africa also seems to be emerging as a new base for Nigerian scammers looking to relocate.

In Ghana, online scamming is not necessarily easy money, as they need to spend hours online converting their marks into customers. The so-called Ghanaian Sakawa boys are not necessarily underworld criminals, but rather young lads looking to earn a good living, as shown in the Vice documentary 'Internet Scamming in Ghana'.

In the documentary, Charles Nelson, who works for Youth Against Cybercrime, says: "Sakawa can be any fraud type. Lottery scam, auction, hit man scam, romance scam. But once you attempt to woo your victim through some spiritual coercion, then it moves from the realm of ordinary fraud to what we call Sakawa here in Ghana."

He says that Ghana has become the 6th worst country for cybercrime, however there are fears that if the government clamps down on scammers, it might have an even worse affect on internet crime, as scamming moves into more organized criminal gangs, using the internet to target victims with more sophisticated blackmail scams.

Malaysia is also becoming a hive for scammers, according to US officials quoted in a report by Reuters, as Nigerians and Ghanaians move on student visas to set up scammer gangs.

Cam-Girls

The Philippines is the cam-girl scam capital of the world. These fraudulent organizations go to great lengths to crowdsource cam-girls. There was even a cam-girl guide uncovered detailing how to perform such scams and get paid commissions for credit card collections.

Sextortion Blackmailers

Most of these scams currently originate in the Philippines and Morocco. The Ivory Coast is also emerging as a new source for these scams.

According to Scam Survivors, some of the worst blackmail crimes have come from these countries. Some high-profile cases include that of Daniel Perry, a young man who committed suicide after blackmailers said they would post explicit content of him they recorded via his webcam.

There have also been isolated incidents of hackers and trolls using similar techniques. These technical experts are able to single-handedly amplify a scam to hundreds of people using scripts, chatbots and other hacker techniques, to uncover highly personal data on a potential victim.

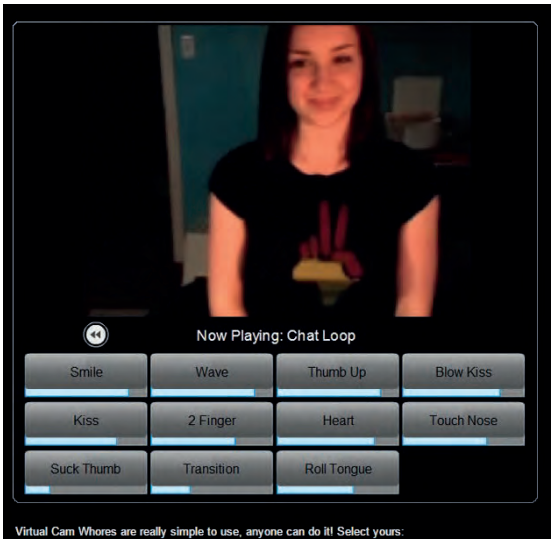
In one high-profile case, Miss Teen USA Cassidy Wolf fell victim to a 20-year-old hacker who went to the same school as her. The hacker, Jared James Abrahams, accessed more than 150 online accounts of over two dozen women in two years. He then blackmailed the women for money.

Virtual Cam Whores (VCW)

Sites like Virtual Cam Whores (NSFW) show how easy it is to use pretty sophisticated virtual video cam-girl animations to dupe users into thinking they are talking to a real person.

Another technique, favoured by Moroccan scam gangs, is to use recorded or stolen redirected footage of the countless cams that run online, such as MyFreeCams and ManyCam.

One way that scammers can access your webcam, as shown in this BBC video, is to inject a piece of code into a web forum, which if clicked by unsuspecting users, can open up their whole computer to be browsed and controlled by the criminal.



Scammers from Russia and Ukraine

The Soviet Union produced some of the best technologists and programmers in the world, and these two countries have become a breeding ground for fraudulent online activity.

Scammers from Ukraine copy stolen pictures from model and porn sites, as well as large unmanaged social networks like vk.com.

Russian scammers tend to use real pictures, and normally pay for women who aren't part of the scam to model for them. These criminals are then known to set up operations called Pods, where they hire somewhere, set up internet and perform the scams, and move on to another location.

These scams generally start with the scammers asking for translation agency costs, then the scammer "falls in love" with the victim and asks for gifts, which progresses into asking for money for visa applications, and then an expensive flight to come and visit their victims.

Scammers based in Russia are also experts at mass mailing from false dating sites, using software like The Bat! to manage scamming on a mass scale. Gmail is currently being used a lot, especially since Google stopped recording the full IPs of their users. Yahoo Messenger has also started to strip user IP addresses, making scammers even harder to detect.

Affiliate Fraudsters and Redirection Fraud

Since dating sites are a fair representation of general population, and have so much demographic information such as location, gender, age, interests etc., some affiliate fraudsters are seeing opportunities in spamming to promote their products - such as the Tinder bot spam. There is even open source software available for people to use.
The other type of affiliate fraud is selling fake and duplicate member leads to dating sites, in return for a fee.

Typically, an affiliate fraudster will create fake profiles from anonymous servers, and receive money from a dating site looking to grow its membership. Sophisticated scammers will even go to great lengths to convert members with fake credit cards, and then doing mass chargebacks. This costs the dating site owners not just an affiliate fee, but also chargeback fees and the cost of internal resources used to manage them.

Redirection fraud is where affiliates harvest emails on dating sites, or redirect traffic from one dating site to another, by pretending to be a member that "prefers" to talk on another site. These sites could be paying the affiliates for traffic, but also could be fake sites gathering masses of emails and profiles, which are then sold en masse to dating sites as genuine leads.

Trending Scammer Phrases

Here are the top 5 trending scammiest phrases in January 2015, according to Scamalytics:

a man who knows how to treat a woman and who understands her deep inside

my dream is to be in arms of right and wise man

trust me i am romantic tender honest intelligent and active lady

forthright and honest i value integrity a sense of fairness

i like to laugh and have been described as having a good sense of humor

TECHNOLOGIES AND METHODS FOR COMBATTING SCAMMERS

In order to detect scammers and fake profiles, there are a number of different methods which sites can use, which all have advantages and disadvantages.

We have collected the methods currently in use by the online dating industry, detailing how effective they are:

Method	Advantages	Disadvantages
Credit card checking	Usually used to check financial transactions, results are reliable when available.	Coverage is limited to countries where reliable data is available, and cost is prohibitive for non-paying customers.
Social Media checking	Identifies the likelihood of a profile being faked.	Most dating clients wish to remain anonymous, and will not willingly allow access. Results are also severely limited by the latest Facebook moves to increase privacy controls.
IP/Network checking	Identifies real location of the user, allowing a check to be made against their profile country. Also allows blocking by IP range or country.	TOR networks and proxies can bypass these.
Device checking	Gets past an IP to the actual device. Identifies fraudsters by checking, for example, the velocity of account creation, and seeing if that device has been used by fraudsters.	Can be beaten by sophisticated scammers using virtual machines. It is also less effective on mobile.
Photo checking	Identifies fraudsters who use a profile image that has been used many times. Sophisticated systems do similar image recognition and share data between sites.	Many users do not initially submit profile pictures. There are also billions of images available on the internet to be copied.
Behavioral analysis	Identifies scammers by analyzing behavior of scammers vs normal users.	Requires specialist developers and experts at big data analysis.
Profile linguistic analysis	Identifies scammers by analyzing word patterns against those commonly used by scammers. System learns from feedback and works with any language.	Requires specialist developers.
Outsourced manual moderation	Can be used to get specialist language skills, or for lower cost.	No retained learnings, difficult to supervise and lower quality moderation than in-house.
In-house moderation	Extremely reactive. Being in-house allows control of priorities instantly. Allows for good quality control.	Can be expensive to hire, train, tool and manage moderators. A high turnaround means some knowledge gets lost when employees leave.
Internal software detection systems	Completely tailored to company needs.	Depends on resource sharing of expensive skilled developers, hardware and hosting; it is a multidisciplinary approach.
External auto-moderation software	Learns on the job, maintains and shares industry knowledge. Up-to-date with latest scam detection techniques and trends; no maintenance, developers or hardware required.	Reliance on outside resource; making sure they are dependable to deliver.
Hybrid systems	Makes most of the advantages, lessens disadvantages and works well for larger companies.	Needs good management to keep multi-system solution running.

DATA SHARING - HOW IT CAN HELP

Sharing data between competing companies for the purposes of tackling fraud is widespread throughout financial services and email providers, but less so in other areas where fraud is nonetheless a problem, such as classifieds and online dating.

However, this is starting to change as dating sites see the benefits of third party data sharing services, who aggregate intelligence and fraud data across multiple sites, and then enable access to it via a central source. Examples range from Maxmind, who provide a generalist anti-fraud service, to device ID-based services such as Iovation and Threatmetrix. Scamalytics provide a dedicated service specifically for the dating industry, including profile data, photos, message text and behavioral patterns. For example, if a "user" behaves similarly to a known bot on a different site, that user will be flagged.

Providing a central database of IP addresses or device IDs is relatively simple, but how does the tech work when you are dealing with something more fluid like messages?

Scamalytics' Dan Winchester:

"We slice and dice each message in a number of ways. Effectively we are looking for three things - longest common phrases which appear in scammer messages but not genuine messages, shorter strings which could be email addresses or chat IDs, and groups of strings and phrases which only become significant in combination. Clearly these are constantly changing, so we update models in realtime to pick up each new wave of bots or organized gangs working to scripts."

Do smaller sites benefit disproportionately from data sharing, given that larger sites are contributing more data?
Winchester says smaller sites are often niche players and can punch above their weight in the specific scams which proliferate amongst their particular demographic:

"A niche Christian site might have as many West African scammers as a large mainstream dating site, due to the fact that there are plenty of genuine West African Christians who lend the scammers undue credibility. We get some of our best learnings from niche sites, and then roll out across the network".

There is a wider industry consideration for data sharing too - each user encounter with a scammer gradually erodes confidence in online dating generally. Just like the insurance industry benefits from collaboratively identifying fraudsters, so does online dating.

Laurence Holloway, co-founder and CTO of Lovestruck:

"It's really important for us to share information about the latest rogue networks, scamming trends and patterns. This "hive mind" is the strongest approach to minimizing the problem. It's also something that the Online Dating Association can help to promote, for the benefit of the whole industry and consumers, too."

Tanya Fathers, co-founder and CEO of Dating Factory:

"There are systems in place like Iovation, Scamalytics, and some payment providers who share databases, that collect the data of scammers on a global scale and give website operators "early warning" score. It helps to catch more scammers based on the experience of other operators, and not just your own."

Jennifer Doherty, Fraud Prevention Team, Cupid Media:

"Using third party technology partners and sharing insights within the industry can help to highlight emerging trends and new technology developments. Scammers target multiple sites and companies and presenting a united front helps discourage scammer behavior."

Ross Williams, co-founder and CEO, White Label Dating:

"Scammers are becoming increasingly sophisticated in the way they operate. There's strength in numbers, so industry sharing means that together, we can analyze scammer behavior and trends more effectively. The more we know about scammer behavior, the better our chance of preventing them from accessing our sites."

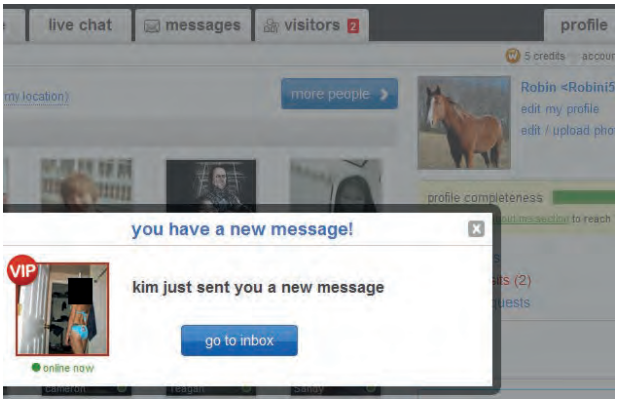
TRUE COST OF SCAMMERS

It wasn't so long ago that you would hear some dating site operators claiming that scammers were actually good for business - they created attractive profiles, sent lots of opening messages, drove engagement and even conversions. Thankfully those days seem to be behind us. Perhaps the turning point was TechCrunch's infamous "horse" test, where journalist Robin Wauters uploaded a profile photo - consisting of a horse - to dating startup WooMe:

"Since I've signed up for the site, again with a horse as my picture and in the middle of the night in the United States, I've been receiving a ton of unsolicited emails, direct messages, pop-ups, live chat sessions and alleged visits to my obviously fake profile by hot women. And I only signed up about 15 minutes ago. Now all I need to do to see who visited my profile or sent me all these private messages, is sign up to become a VIP WooMe member ($24.99 per month)."

Later that year, WooMe was acquired by Zoosk in an "apparent fire sale", despite $20m of investment from the likes of Index Ventures.

So clearly there is an enormous reputational risk in allowing scammers to run amok on your dating site. But what about a quantifiable business cost? Something dating sites can use to allocate resources to the issue, knowing they should get a payback, and the timeframe in which that payback will likely happen.



Scammers cost dating sites in three main areas:

1. Direct costs of chargebacks and affiliate fraud

These direct costs are relatively easy to quantify. A proportion of chargebacks will be caused by genuine-but-disgruntled users, so called "friendly fraud". The rest are scammers or fraudsters checking cards. Work out the proportions of each, and by deducting scammers and fraudsters you can see how many chargebacks you can eliminate and then work out the cost savings in reduced chargebacks and lower banking fees. Scamalytics research says that typically around 50% of chargebacks are down to "friendly fraud" and the other 50% is theoretically preventable depending on how good your anti-fraud measures are.

Affiliate fraud is pretty easy to calculate after the fact. Looking at a period where all the data has come in, you should be able to work out which affiliates were fraudulent, and calculate the cost of paying out to those fraudulent affiliates for the period in question.

2. Decreased LTV through lower conversions and higher churn

An exit survey is the best way to attribute a cost here. When users leave your site, survey a sample to ask why. Include reasons such as "no longer single", "too expensive", but one reason should be "I encountered scammers and fake profiles". A proportion will not answer the survey, be sure to exclude these from any calculations. Once you have some data, you can start working out the impact on LTV. For example, let's say 12% leave due to scammers, your average subscriber stays 90 days, and the 12% leave before paying for a second month. This means 12% of your subscribers are paying for 30 days when they could be paying for 90 days, meaning you are getting only one third of the potential revenue from those 12%. This equates to 8% of total potential subscriber revenue being lost to scammers.

You can apply the same technique to registered users who leave before converting.

3. Opportunity cost of having your development team tied up battling scammers instead of progressing your product

Plenty of dating startups neglect to put a cost for scammer-prevention in the business plan, and plenty more find that their original estimates were way off the mark - fraud can be characterized as an arms race, which makes it very difficult to predict resourcing requirements accurately. This means unplanned investment, which diverts money from the original plan. If your competitors are pushing out features and supporting more and more devices, whilst your dev team are bogged down fighting fraud, then you have a problem which impacts the very viability of the business.

You can attribute a cost to this simply by looking at the unplanned expense of dealing with scammers and fraud. How much extra have you had to invest, and what would be the return on that investment if you could spend it on product?

These costs need to be balanced against the direct costs of fighting scammers:

1. Increased moderation overhead

Whilst tech can catch a large percentage of scammers, you are likely to have a proportion which you want to escalate to your moderation team for a manual check. Just as each missed scammer represents a cost, each false positive is also a cost - an acquisition which will never convert.

2. Dev resources to build out scammer detection and moderation systems

It is typically cheaper over the long term to have computers detect scammers than rely solely on humans, but the tech needs to be built, or bought and integrated, and generally there is also some integration into the moderation system required as well.

3. Cost of third party services, and integration of those services

Almost all dating sites use third party systems, even if it is just an IP lookup service. These third party systems must be paid for and integrated.

We can see that it is reasonably easy to work out the cost of tackling scammers. But we can also see that it is possible to work out the cost to the business of not tackling those scammers. These numbers can be worked into the business plan, allowing resources to be properly allocated, with the surety that both scammers are being tackled and revenues are increased.

George Kidd
Chief Executive of the Online Dating Association

"I believe scammers pollute the online services they try to use to attack. I do not buy the argument that having dodgy people on a service somehow makes the service feel busier or more vibrant. I am not sure what the best offline equivalent is, but the idea that a football crowd is better if topped-up with a few hundred cardboard cut-out fans or Stepford Wives going around and around a supermarket makes me stay longer or buy more is doubtful. Would a bar really celebrate having a dozen pickpockets in the place in the hope it seemed buzzing? Ours is an amazingly creative industry, constantly coming up with offers, events and ideas to improve the user experience. That is where the effort lies."

CONCLUSION

Scammers and fraudsters will likely always be an unwelcome aspect of online dating.

These criminals from around the world persistently find new ways to dupe singles, either by infecting the hottest dating apps, harnessing new technologies for the latest scams like sextortion, or circumventing security measures designed to block them.

However despite this, there is meaningful and effective action that can be taken to diminish their impact.

Dating sites must improve their securities, keep up with the latest trends, and educate their members to report fraudulent profiles.

And this work has to be done with the support of law enforcement agencies and regulatory bodies, who must do what they can to catch these criminals, and increase awareness about their tactics.

Improving the trust in online dating is now more important than ever, as its influence and popularity continues to grow throughout the world.

And as this happens, and with security and privacy at the forefront of consumers' minds, those who do not ensure their members are safe, will likely struggle as the industry moves forward.

We would like to thank everyone who contributed to this report by giving their insights on this important topic.

And a big thanks also goes to our sponsor and collaborator Scamalytics.

We hope you enjoyed the report, and thanks for all your support.

Simon Edmunds
Editor
Global Dating Insights

Scamalytics

Stop Scammers Automatically

Scamalytics helps you automatically and accurately stop dating fraud like: chargebacks, affiliate fraud, camgirl fraud, redirection fraud, romance scams and fake profiles.

If you'd like to discuss how Scamalytics can protect your users, your reputation and your revenues, please get in touch.

Contact us at info@scamalytics.com for a FREE 60 Day Trial

SIMON EDMUNDS, EDITOR
E: EDITORIAL@GLOBALDATINGINSIGHTS.COM
M: +44 (0) 7770 525 242
T: +44 (0) 20 3318 8588
TWITTER: @GLOBAL_DATING

ADDRESS:
116 PALL MALL
LONDON
SW1Y 5ED

SIMON CORBETT, FOUNDER
E: SIMON@GLOBALDATINGINSIGHTS.COM
M: +44 (0) 7974 093 944
T: +44 (0) 20 3318 8588
TWITTER: @GLOBAL_DATING