Data breaches are creating a new breed of online scammer, write Ramon Lobato and Julian Thomas

Before the fall: Noel Biderman, chief executive of Avid Life Media, owner of AshleyMadison.com, speaking at TEDxWaterloo in March 2013. TEDxWaterloo/Flickr

Fallout from the Impact Team’s Ashley Madison hack continues, as millions of subscribers to the online hook-up service – and their partners and families – come to terms with one of the largest data breaches in history. Last week, Canadian police reported two likely Madison-related suicides. This week Noel Biderman, CEO of Toronto-based Avid Life – the pariah company behind Madison and its sister websites Cougar Life, Down Low and Established Men – finally stepped down. Like a train wreck, the unfolding saga makes for compulsive and unsettling viewing.

One of the creepier developments has been the appearance of internet entrepreneurs seeking to profit from the privacy breach in one way or another. Studying these business models provides insight into the harvesting of personal information online, both inside and outside the law.

At one extreme there are the blackmailers, whose appearance has been both swift and unsurprising. Madison users are now being individually targeted with threats to expose them to their Facebook friends unless they pay up in seven days, via emails that read, “If you would like to prevent me from sharing this dirt with all of your known friends and family (and perhaps even your work too?) then you need to send exactly 1.05 bitcoins [about A$340] to the following BTC address…”

Then there are “removal” services that have appeared, promising to wipe your name, credit card number and sexual preferences from the internet. Obviously these services don’t work – the Madison data has circulated widely across the web, custom search sites and BitTorrent, so removal is impossible – but plenty of operators will happily take your money anyway.

One example is Trustify, an online marketplace for hiring private detectives. Trustify used the Ashley Madison data to set up its own search engine, inviting people to check if their email addresses (or those of partners, friends and associates) were in the leaked data. It then sent out “notification” emails to the addresses in question, with a subject header of “Your Boss Might Know,” suggesting they hire a Trustify private detective to protect their reputation.

This kind of business model brings to mind earlier precedents such as the photo-takedown scam, in which websites publish compromising images and then offer a “service” to have them removed, via a separate (but linked) site. This trap came to light in 2011 when Wired uncovered a mini-industry of American mugshot websites that were exploiting freedom-of-information laws in certain US states to collect and publish police images of people charged with driving under the influence and minor drug offences, then demanding up to US$399 for their removal.

Similar scams have been run on “revenge porn” sites, such as UGotPosted.com and its sister “removal” site Changemyreputation.com, which charged desperate women extortionate sums to scrub their images from the public record.
The Ashley Madison case is complicated by the fact that Avid Life was running its own identity racket. As Ars Technica revealed a while back, Ashley Madison customers wishing to delete their profiles were offered a “full delete” or “ghost erase” service for $19, which promised to remove all data. But we now know that the personal info remained on Avid’s systems even after the fee was paid.

On the other side of the fence, entrepreneurial cybersecurity firms have been using the Madison saga as a platform to promote their services. News reports are quoting security experts keen to hawk their services to government agencies and companies nervous about Madison-exposed staff being blackmailed for confidential information. This is completely legal, of course, and probably useful given the scale of the leak. But it follows the same logic: a privacy threat is identified and a commercial “solution” offered in response.

The Ashley Madison case provides us with a glimpse into an obscure world – an industry dealing in the fabrication, extraction, circulation, analysis and control of personal identities and reputations. While much has been written in recent weeks about the morality of cheating websites, the ethics of this commercial information harvesting have yet to be fully explored. All this suggests an interesting future for online hook-up sites, and their customers, in the years ahead. •