SEX, LIES AND THE MISSING VIDEOTAPE

TWO YEARS AGO, WE REVEALED HOW THOUSANDS OF BRITONS WERE FALSELY BRANDED PAEDOPHILES. NOW **DUNCAN CAMPBELL** FINDS THEY WERE VICTIMS OF CRIME THEMSELVES

In 2005, *PC Pro* revealed how computer evidence used against 7,272 people in the UK accused of being paedophiles had been founded on falsehoods (*see issue 130, p152*). The misleading evidence, which claimed that every user of a Texas porn portal had to click on a banner advertising child porn to access illegal websites, was withdrawn last summer. "It's specifically not alleged that [the accused] would have ... seen a banner saying 'Click Here Child Porn'," a British court was told.

The climb-down came too late for many: between then and now, the death toll of those who have killed themselves under pressure of the investigations in "Operation Ore" has risen from 33 to 39.

Hundreds of police raids across Britain found no evidence that many suspects possessed, or were even interested in, child pornography. Because of the huge volume of computers and disks seized for examination, police high-tech crime capabilities were reportedly crippled for years.

Now, *PC Pro* can exclusively reveal that not only did police evidence in Operation Ore pretend users had asked for "child porn", but that many of the Britons who have been publicly branded dangerous paedophiles were merely victims of systematic credit card fraud – some of it run by a Mafia crime family – and had never subscribed to the websites.

The secret videotape

Three months after the *PC Pro* report was published, documents obtained from the US revealed the existence of a videotape showing what really happened on the website in question, Landslide.com. On 28 April 1999, a Texas detective, Steve Nelson, had decided to record what happened when visitors logged in to the Landslide website. With the help of Microsoft, he connected a video recorder to his PC. The resulting VHS tape of Landslide.com was allocated exhibit number SN-A-1.

A minority of sex sites accessed through Landslide offered horrific child pornography. Videotape SN-A-1 became the US government's first exhibit in the successful October 2000 trial of Thomas Reedy, Landslide's owner and manager. Court transcripts from the case described the videotape and confirmed what *PC Pro* reported – there was no "click here" button on the Landslide first page.

Two years later, in a statement taken by British police, Nelson's story had changed. It was claimed that the button was on the front page, and was an essential step to accessing any site.

The US court transcripts, exhibits list, and a copy of videotape SN-A-1 were brought to Britain in 2002. When *PC Pro* asked the Crown Prosecution Service (CPS) if the video tape had ever been officially produced as evidence, it issued a statement claiming: "SN-A-1 is a video tape produced by US Postal Inspector Steve Nelson. In cases in which it is relevant it has been exhibited and made available to the defence." Nelson is a detective, not a "Postal Inspector", and he has never given evidence in a UK court.

Nor has the CPS been willing to disclose that, since the end of 2002, the police had evidence that many of those they called paedophiles were, in reality, simply victims of internet credit card fraud.

Carding rackets

Evidence of the credit card frauds – revealed exclusively here – has been found on copies of six computer hard drives that were seized from Landslide by police, the FBI and government agents. Copies of the hard drives were made for the Landslide trial. Late in 2006, the copies were flown to Britain to be examined by defence computer experts (including the writer).

As soon as the hard drive copies were opened, it was obvious that Landslide's activities had been riddled with fraud. Independent computer expert Jim Bates, of Computer Investigations (**www.computer-investigations.com**), said "the scale of the fraud, especially hacking, just leapt off the screen".

The previously undisclosed computer files showed that Landslide had been plagued by a range of credit card fraud rackets, known in the industry as Card Not Present (CNP) frauds. CNP transactions occur when the cardholder, or someone pretending to be them, provide their card and personal details over the internet, or by phone. The people who do it call it "carding". CNP fraud has increased exponentially over the past decade to become the largest type of card fraud in the UK.

DUNCAN CAMPBELL
An investigative journalist, who here writes exclusively for PC Pro following his involvement as an expert witness in several Operation Ore investigations.

Operation Ore exposed

Operation Ore is the UK's biggest ever IT crime investigation, but expert witness Duncan Campbell reveals that many prosecutions were founded on falsehoods

PC Pro exposed Ore's flaws in 2005.

"Carding" has been carried out over the internet in international black markets since the mid-1990s. Organised groups with closed websites and chat groups, such as CardersMarket, DarkMarket, TalkCash or TheVouched, trade stolen credit card data in bulk "dumps", pricing it according to its potential fraud value. Prices advertised in their net postings range from $30 for a single "virgin" (unexploited) Visa Gold card to $10,000 for a bumper file of 4,000 stolen American Express card and user details – just $2.50 each. A typical dump of British credit card holders' stolen data contains not only card numbers and expiry dates, but name, address, date of birth, email, personal password and even mothers' maiden names – everything needed for complete and convincing frauds.

"Phishing" was a word nobody had heard of in 1999, and the way the carders harvested data from their victims was simpler than today's carefully crafted and deceptive spam emails. They advertised cheap adult sex sites on the internet, and offered access in return for a credit card payment, perhaps as little as $1.95. A customer who signed up had to provide his or her name, address, card details, and email address and password. That was all the carders needed. The data collected could then be reused or traded online with other fraudsters.

Carding through phoney (or real) porn sites is a simple way to earn millions because nothing has to be delivered. Operating out of Indonesia, Russia or Brazil, many of Landslide's webmasters appeared to have obtained and swapped lists of stolen cards and charged them up through different portals. Transactions were usually for repeated small amounts of less than $50.

Many victims were charged numerous times by websites they'd never heard of. Some noticed, and applied for "chargebacks" – refunds provided by the bank when unauthorised transactions have taken place. Most people didn't notice or couldn't find out how to get refunds.

Under British law and the Human Rights Act, lawyers and experts are supposed to have the right to check all the evidence that might be relevant to a defence case. But since Operation Ore began, the police unit responsible has refused to allow full checks on the computer evidence by independentexperts, and has sought to restrict access to

police-approved experts only. The CPS insists this statement is "incorrect" and that "it is always open to the defence to apply to the court for access to any exhibit or any item of unused material".

Computer experts employed by the police have claimed in court cases they could find no evidence of hacking or fraud. "Did you actually go looking for fraud?" Dr Sam Type of Geek Ltd was asked during one case held at Northampton Crown Court. "No I didn't, no... I haven't specifically looked for it," she replied.

THE COMPUTER MANAGER

After Brighton computer manager Brian Cooper bought bike parts from the US over the internet, his card details were used by Indonesian fraudster Akip Anshori to sign him up to porn websites. As police searched his home, his wife Gill recorded a diary and her shock at being told her husband was a risk to their children.

The family's computers were kept for six months. Nothing was found. Cooper pointed out that he had complained about the frauds at the time. He was never charged with any offence, and yet the police initially refused to apologise.

After obtaining copies of his computer records, Cooper says the records should have been detected as fraudulent. He'd been signed-up using the obviously spoof email addresses a@a.com. In April 2006, Sussex Police apologised for subjecting him and his family to distress and "an investigation which clearly was unnecessary".

The Soprano connection

The American Mafia ran the largest credit card porn site racket, which the FBI claims netted members of the Gambino family over $230 million between 1996 and 2001. The Mafia scheme was audacious and ingenious. Their honey trap websites offered "free tours" of porn sites before entering. The sites asked visitors for credit card details, supposedly to prove their age. In fact, their cards were then charged up to $90 a month for non-existent subscriptions to porn sites.

It might be hard to imagine falling for such a ruse now, or not checking credit card statements afterwards to look for abuse. But, across the world, tens or hundreds of thousands of people did. Some British victims of the Gambino family internet fraud later became targets of Operation Ore. On 9 January 2006, Gambino family capo Richard Martino and his brother Daniel were ordered to pay $6.4 million and sentenced to five years in jail without parole.

Top city banker John Adam was one of the Mafia's many fraud victims. During 1998 and 1999, his family credit card was charged repeatedly by Gambino internet organisations.

The stolen data was shared with other fraudsters. In June 1999, Adam's card was used twice more to pay for sites run by Arief Dharmawan, one of Landslide's top webmasters – and a child porn merchant.

Seven years later in May 2006, Adam, a pillar of society, stood aghast as police entered his home and trawled through his family's intimate possessions. He says

THE NATIONAL HERO

Emergency consultant Dr Paul Grout of Hull was hailed as a national hero when he led medical teams treating victims of the Selby rail disaster. But his career collapsed when his card details were fraudulently used by Indonesian webmasters Michael "Miranda" Yamin and Akip Anshori.

Operation Ore police invaded his house "like stormtroopers" in October 2002, his wife Susan later told the BBC. The family then endured "18 months of sheer hell". Nothing was found in the Grouts' home or on the doctor's computers. Nevertheless, he was charged with "incitement" to distribute indecent pictures of children.

Two years later, Hull judge David Bentley threw the case out. He told the police that their evidence was "utter nonsense". Instructing the jury to acquit the doctor, he invited him to "get back to the business of saving lives".

Some British victims believe their troubles began after they bought bicycle parts over the internet

that police officers "sneered" when he and his lawyers told them about credit card fraud. "They said they had never heard of it happening," he told *PC Pro*. Only after a two-day High Court case last September did the police agree that Adam was above suspicion and apologise to him.

Ironically, even as the UK police launched Operation Ore in 2002 in the belief they had obtained a unique hit list of paedophiles, the FBI had closed in on the Gambino family scam. While the successes of Operation Ore attracted publicity, the British government issued a warning that "Subscribers to 'adult sites' find that additional and unauthorised withdrawals are made against their credit cards". The left hand of the police clearly didn't know what the right was doing.

Card and personal details weren't only obtained from sex website scams, but also from orthodox online traders. Some British victims of card fraud who later suffered from police mistakes in Operation Ore believe their troubles began after they bought bicycle parts – or even a honeymoon hotel stay – over the internet or on the phone from the US.

Hackers who broke into insecure trading sites stole vast quantities of personal credit card data to use for fake porn site sign-ups. Hidden away on Landslide's computers were 54,348 sets of stolen credit card information, including information on dozens of UK residents. The data appeared to have been stolen en masse from a Florida-based luxury goods company, in the form of Microsoft Access databases of its complete customer records. Some of the stolen cards were later used to pay for porn websites operated by Landslide. The company whose customer data was stolen, Levenger Inc of Delray Beach, Florida, has declined to comment.

The minister and the FBI

Landslide computer files record that on 10 May 1998, Jason Little of New Orleans paid $49.95 to Landslide using a Bank of Ceylon credit card. The card really belonged to Mangala Samaraweera, the Minister of Telecommunications and Media in Sri Lanka. He called in the country's Chief of Police, who complained to the FBI. It was the first omen as to the nature of much of the business going through Landslide.

An international FBI investigation soon established that the minister had been carded both by Landslide Inc and by another US scam portal, Dakotah Marketing and Research (DMR). A year later, DMR collapsed amid a mountain of millions of dollars of chargebacks demanded by credit card firms.

According to personal emails found on the home computer of Landslide Inc's owner, Thomas Reedy, he first spotted systematic frauds late one night in August 1998. "We were very lucky," he told a friend in an email, "I was running over the logs late one evening and saw something funny." What he noticed was that streams of different credit cards were being signed up in batches from the same internet address to the same website. Reedy quickly traced the source of the traffic to Pakistan-based webmaster Imran Mirza and his "Rare Nude Celebs" website. They "had someone or someones run the cc#'s thru (sic) to credit their site with funds," Reedy wrote. "In just the three days that they were doing it to us, they ran over $14,000 worth of charges thru."

The computer files reveal that Reedy then set out to protect himself against fraud by setting up a new web service called Badcard.com. He wrote software to block the armies of carders by trapping card numbers coming from the same internet address, and drew up checklists of addresses and card numbers he suspected were in the hands of criminals.

Optimistic that he had cut off the web cheats, Reedy launched an expensive new web service called Keyz in 1998. Unlike his previous adult services, where a user paid a one-off fee to access many porn sites, Keyz charged up to $29.95 for access to a single site. Reedy offered to pass 65% of the proceeds to webmasters and promoted the new service with the slogan: Keyz will "turn your website into a MONEY machine".

The Landslide computer records seen by *PC Pro* show that Keyz was a money machine – but for fraudsters. Reedy didn't notice, and bragged about the Badcard security system to other companies: "Landslide, Inc is so confident that we can reduce the number of chargebacks at your site we over (sic) a full refund if you are not completely satisfied. What do you have to lose?"

"Everything," was the answer. Reedy's Badcard system didn't work well enough. Fraudsters started switching internet addresses with each new, false sign-up. Within nine months, Landslide was dead in the water.

↑ The Who star Pete Townshend was arrested and had his computer seized during Operation Ore.

THE WEDDING VIDEOGRAPHER

Wedding videographer Jeff Chapman first learned of Operation Ore when police arrived at his north London video shop and cleared it of all his videotapes and computers. His card details had been found on Landslide's computer records.

After months going through what the police hoped was a treasure trove of child porn, they found only professional recordings of weddings. But he was then charged with making images of children, which had been found on a computer used by a former employer.

The charges were dropped in 2005 when prosecutors discovered the police had withheld critical evidence. Chapman is now suing Hertfordshire Constabulary.

Reedy is now in US federal prison, serving a 180-year sentence for allowing Keyz to be used for child porn trafficking.

Wide-scale fraud

Following the launch of the Keyz service, Landslide's revenues soared from $162,000 a month in September 1998 to $824,000 in July 1999, according to financial files stored on the company's computers. But a close look at Landslide's internet records reveals where that "revenue" was coming from.

Although many webmasters were trading legitimately, the biggest business was being conducted by credit card fraudsters. Topping the league were Indra Imansjah, Arief Dharmawan and Michael Yamin, who traded under the pseudonym "Miranda". They were part of a gang of Indonesian webmasters. More than half of the money Landslide took from card owners was paid to the Indonesian ring. Dharmawan and his colleagues were in the business of supplying extremely unpleasant pornography over the internet, some of it depicting young children being raped and abused. But the undisclosed computer evidence shows they were also in the simpler and less risky business of card fraud.

The number of people signing up for the Indonesians' child porn websites shows a strikingly common pattern. Yamin had a dozen websites signed up to the Keyz service (in different names) in January 1999, but by March he had only two paying customers. By May, that figure had suddenly shot up to 7,000 subscribers, earning him $137,000 in fees. Other websites run by the trio showed similar traffic surges.

Had the world suddenly woken up to child porn? "I don't think so," says Ross Anderson, Professor of Security Engineering at Cambridge University and an expert in banking frauds. "The Indonesians could simply have bought in lists of credit card numbers to exploit". Doing this on sites that contained child pornography was a "clever twist", Professor Anderson adds.

Whereas legitimate sites tend to receive steady levels of new members, crooked sites only received subscriptions when the webmasters or their accomplices feed in new credit card numbers. Sign-ups to these Indonesian sites happened only in clusters on scattered days.

The consequences of the many frauds soon became obvious in Texas. According to a post mortem study in August 1999 by Landslide's chief financial officer Kean Songy, the level of repayments and chargebacks prompted by unauthorised fraudulent transactions rose steadily, reaching nearly 10% in July 1999. On Landslide websites that computer records show were simply vehicles for fraud, 90% of the people cheated never complained. The true level of card fraud involved in Landslide and Operation Ore can never be known. But it suggests that only one in ten victims complained about the fraud, and the likely total level of fraud was well over 50%.

Computer expert Jim Bates spotted an obvious way of separating frauds from genuine porn purchases on the Landslide website. One important evidential file is a giant 424MB container simply called "Access". This was a complete log of all recent internet activity. It recorded when credit cards were signed up and charged. Critically, it also showed whether the person putting in the card details had gone on to visit the porn site their card had paid for. Bates' analyses found that not only did thousands of the supposed porn buyers not go to get their porn, many Keyz sites had been set up purely for fraud.

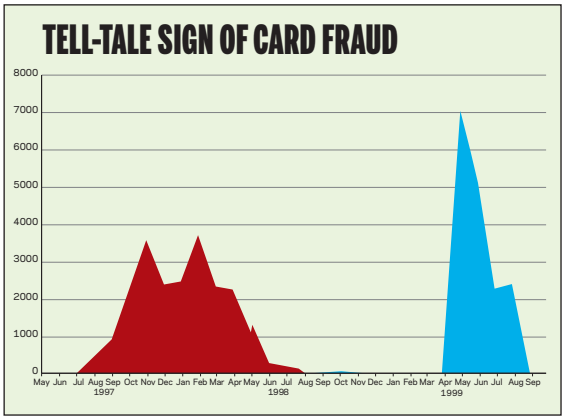
Top of the list of spurious websites was "Keyzsexyplace", set up on 4 April 1999 by young Brazilian hacker Antonio Francisco "Nino" Tornisiello, from Piracicaba, near Sao Paulo in Brazil. Tornisiello penetrated Landslide's non-existent security screens, copied their programs and then constructed a high-speed fraud system to fire streams of stolen credit card information past the sign-up forms and fraud checks devised by Reedy and his programmers. By the time Landslide collapsed, he'd logged 3,181 sign-ups, most of them using stolen British credit card information.

"Tornisiello's hacking stood out like a sore thumb," Bates told *PC Pro*. He took all the personal information, coded it as a single string and fired it in batches at Landslide's upstream processing. "The police experts couldn't have failed to notice it, if they were competent, but they claimed they saw nothing," Bates says.

Among Tornisiello's many British victims were prominent computer programmers and businessmen, some of them readers of this magazine. Some of them were lucky. The Operation Ore police haven't got round to knocking at their doors – yet. Nevertheless, their names are now falsely listed in police files as suspected child abusers.

When confronted with our evidence, Tornisiello admitted to *PC Pro* that his Keyzsexyplace website had been a sham that held only "a page with pictures of celebrities I found over the internet. It was nothing to do with child pornography."

Tornisiello said he was "choked" to learn that, because of his actions, innocent people have been accused of paedophilia. "Everyone has something in their past they regret," he said.



The sudden peaks in sign-ups to the Miranda website are indicative of fraud.

Fraudster Antonio Tornisiello now stars in a rock band.

Pseudonyms have been used in this report to protect the real identities of "John Adam" and "Jeff Chapman".

THE MUSICIANS

Rock stars Robert del Naja of Massive Attack and legendary The Who guitarist Pete Townshend were both arrested in 2003, after the police had leaked their names to the tabloid press. Both men's names are listed on Landslide records as signed up to Keyz websites. But the police never had any evidence that the websites concerned – which are shown as "Alberto" and "Spermed" – had anything to do with children. Nothing was found on their personal computers.

The investigations against Mr del Naja were dropped within a month due to insufficient evidence. But the police didn't tell Townshend that their entire evidence against him was a single entry made on Landslide on 15 May 1999 for the purchase of the Alberto website. Under pressure of the media filming of the raid, Townshend appears to have confessed to something he didn't do. He was cautioned and his name was placed on the sex offenders register.

The del Naja probe was dropped.

Ironically, in April 2006, the Home Office launched the child protection agency CEOP with del Naja's song, *Teardrop*. Head of CEOP James Gamble, the person responsible for Operation Ore, told the press "I didn't choose the music".