Thief of Hearts

Online dating scammers leave behind dashed hopes—and empty bank accounts

Femmes fatales, swindling Lotharios and romantic con artists are practically as old as time. They say all the right things, play all the right games, dupe unsuspecting innocents into developing real feelings for them—and then somehow, in some way, get money out of victims. Online dating scams are only the latest incarnation of the emotional swindle.

In the face of a weak economy, many singles are choosing an online dating service as a higher-yielding alternative to a singles scene—and a bargain, considering that even sites with a membership fee (usually $20 to $35 per month) beat a hefty bar tab.

Most dating sites have reported swift and steady profit gains and, according to a 2010 Nielsen poll, one in four adults has tried online dating. Those on the U.S. Internet dating market are projected to spend $932 million in 2011—up from $469 million in 2004. *Continued on page 3* ▶

Smartphone, Dumb Security

So your phone can edit a video, but can it protect your data?

Sure, smartphones make communication easier. Part central computer, part electronic valet, they make troves of information—from *War and Peace* to your grandma's birthday to a restaurant reservation—available at the touch of a fingertip. These mighty minis even have the power to change lives: Smartphone data has been used to clear accused people of serious crimes, and police have used iPhone geomapping to track down stolen cars with the device still in them. Smartphones also keep users in touch with friends, relatives—and, unfortunately, hackers and thieves. *Continued on page 4* ▶

Living the Dream

During his 1988 vice-presidential debate with Lloyd Benson, Dan Quayle waxed eloquently about the limitless opportunities in America. He reminisced about the time his grandmother put him to bed and said, "Danny, you can be whatever you want to be." Never underestimate the value of inspiring words from loved ones. Also never underestimate the inspirational value of a $650 million trust fund. He had both. And he obviously took those words to heart and almost hit the brass ring—for a four-year period he was but one heartbeat away from becoming president of the United States. Inspiration, love, money—all the elements of Valentine's Day, yes?

When I think about Valentine's Day, I am inescapably drawn to the subject of social networking and dating sites—the lure, the romance, the mystery and the danger. To quote Rod Serling, the creator and chief writer of *The Twilight Zone*, "Submitted for your consideration," this scenario: Across the cyberuniverse, sitting in a dark room, in front of a computer monitor, anonymously typing to someone known or unknown ("the mark"), the writer can morph into anyone—or anyone the mark wants them to be. And oftentimes, the writer can get the mark to do things the writer wants them to do—things they ordinarily wouldn't do—because the writer is giving the mark the dream they want or need to dream.

There was a song from the Prohibition era entitled "How Could You Believe Me When I Said I Loved You When You Know I've Been a Liar All My Life." Imagine the luck of the draw if you picked that title in a charades game.

Valentine's Day is all about the dream. But these days, the dream seems more about florists, jewelers, restaurants and hotels than predestined lovers. And the dream—or the perversion thereof—is what this Valentine's Day edition of our newsletter is all about.

This month we focus on the schemers who take advantage of the dreamers—when the heart is not "a Lonely Hunter," but rather the hunted.

We also look at the dangers posed by the ubiquitous smartphone—email and texting gateway to the lovelorn. We provide tips on how best to prevent your handheld, ear-friendly minicomputer from sharing your love letters and poems with those who are passionate to get past the prose and put their hands on every other byte of your sensitive personal information.

We discuss a case in which Identity Theft 911 showed a little love to a nonclient and helped her resolve a horrible situation that almost destroyed her life.

Finally, after Hailing and Hissing about a few issues, we talk about how to better protect yourself from identity theft if you "Leave on a Jet Plane," or any other mode of transportation, and move to another home.

So think of this issue as our heartfelt gift of identity-management flowers or a box of fraud-prevention chocolates. It is our profound hope that the better we can help you insulate yourself from exposure to identity theft, the more time you'll have to stop and smell the roses, get a date—or spend some quality time with loved ones.

Adam K. Levin
Chairman and Founder
Identity Theft 911 LLC

In this issue...

Features

Departments

Thief of Hearts from page 1 ▸

It's too big a party for dating defrauders to pass up. All it takes is the trust and vulnerability of one victim, and a thief can become a few thousand dollars richer—while operating the whole scam from the comfort of an Internet cafe.

"The more known a site is, the more people are on it perpetrating fraud," explained Victor Searcy, manager of fraud operations at Identity Theft 911. "Criminals and noncriminals alike know what Coca-Cola is. eHarmony and Match.com are the Coke of dating sites, so that's why criminals target more victims there. It's a numbers game."

A typical dating scam might play out like this: You meet someone who's immediately charming and says all the right things but lives far away, possibly out of the country. "You're such a good man, you'd make a wonderful husband," a woman might coo to her male suitor. Another line might read, "I know we've never met in person, but I feel like I love you." The sentiments will be sweet and romantic but strangely generic and can be accompanied by gifts or flowers. The con artist will say he wants to come visit—if only you could wire him some money for the trip. Or she might even ask the victim to book a plane ticket and, having sent her mark a fake photo, walk right past him at the gate. Voilà—a free trip to his hometown.

Scammers can spend months nurturing an online relationship before asking for money. "Sometimes they'll start small, to see what they can get, and keep going until the well is dry," said Eduard Goodman, Identity Theft 911's chief privacy officer. "They won't ask for $10,000 up front. They build up to bigger amounts, knowing that some people are just lonely enough to hold onto a little string of hope."

The lonelier the prospective victim, the greater the likelihood they'll fall for the scam. "They're the ones who engage," Goodman said of the lonely hearts. "They'll accept packages from strangers. They'll say, 'I'd love to help you.' [For the scammer] it's the shotgun approach—fire off a bunch of shots and see what hits." The elderly are easy targets, as are those on a niche dating site, such as a religious one, where they might inherently trust those who share their faith.

After the courtship has been underway a few weeks, there's inevitably an "emergency." The crook says he's out of the country on business, someone has stolen his wallet, and he doesn't have enough money to return to the States.

"Can you wire me $1,000?" he'll ask. Or, inexplicably, he'll offer to have a friend send the victim a check for $3,000, if the victim could send him back a check for $2,000—and keep the difference.

Even if the check clears, it could have been altered—the payee may have been changed—and it has the potential to be returned within one year of the deposit.

Unfortunately, there's no stopping online dating scams, particularly as the technology and the industry grow. The sites themselves can ban a repeat offender from posting his or her profile to its members, but what's to stop the perpetrator from simply rejoining with another name and email address? And, with fraud in amounts under $10,000, it's hard to get the local police or the FBI to pay attention, especially if it's international.

"The biggest problem," Goodman said, "is that this type of fraud is hugely underreported. People don't want to tell their friends and family, 'I got scammed by someone I thought was in love with me.' It's embarrassing and humiliating." The further someone is from the mainstream dating world, the more vulnerable they become.

For the millions of honest people simply hoping to meet a mate online, the best plan of action is to pay attention to the warning signs (see box) and cut off the relationship before a scam happens. But most important, daters should never let their hopes and their hearts outweigh their instincts.

"Trust your gut," Searcy said. "Almost everyone this happens to says, 'I always felt something was off.' If a stranger is asking you to do something you wouldn't do for someone you know, don't do it." •

How do you know he likes you for your money?

1. Does your prospective date make generalized statements such as, "I feel so close to you," instead of addressing specific topics you've mentioned in your emails?
2. Do they reveal very little about themselves? Are they vague about what they do and who they are?
3. Do they have poor spelling or grammar or use British spellings of words (such as "favour"), even though they claim to be American?
4. Does the profile photo look too good to be true?
5. Does something just seem "off"? Are the requests for money convoluted—such as, "I'll have a friend send you a check, wait until it clears, then you send me $2,000 and keep the rest"?
6. Are you given a series of different phone numbers to call or addresses in other countries?

Smartphone, Dumb Security from page 1 ▸

What does all this mean to the average consumer or business user? Simple: It's time to stop thinking of these petite but powerful machines as phones and start protecting them like computers.

There are various security options—and weaknesses—in the most popular smartphone models and apps, but a few basic tips and tricks can immediately up your phone security game.

First is simple common sense. What information is on your smartphone? If you access a Gmail account or online banking, are the passwords saved into the apps? Do you read sensitive business documents on your phone? Do you have images of your Social Security card or passport? Such files can be a boon if you lose physical documents overseas, but what if your phone is stolen? And those falsely accused folks cleared of criminal charges? It was *erased* data that saved them. An expert (good guy or bad) can recover voicemails, texts, emails—any kind of key swipe—from as long as 12 months ago.

The first step to securing a smartphone is to make a physical list—pen and paper, people—of all accounts and documents (or types of documents) you access on your phone. Remove anything nonessential—do you really need that client roster loaded with billing info?—and cross it off the list. Put that list in a safe place, such as a home office safe or safety deposit box. If your phone is lost or stolen, you'll be glad you have it.

Then remove all stored login names and passwords (some of which may have been autosaved by your phone) for apps and web pages. The extra four seconds you spend manually entering that information at each login will save hours of headache if the phone is compromised.

The second line of defense is encryption, which essentially scrambles the data on your phone's drive, only allowing access if the correct code is entered. It's more sophisticated than a standard phone lock, because the data on the actual drive is changed—thieves can't simply pull the drive or run a password breaker to access it. (Even still, you should always have your standard phone lock ON.) Most smartphone operating systems—iPhone, BlackBerry, Android—offer encryption options.

Your third step is third-party security apps. Lookout Mobile Security is a good starting point for Android, BlackBerry and Windows Mobile users. The free package includes an antivirus application, automated data backup and a device tracker. iPhone users can pay for MobileMe. But don't let tracking programs fool you: They all need to be activated and running in the foreground to work. If your phone is off or the app isn't running when the phone goes missing, it's not much good. (And surely a smart thief knows about the $20 signal-blocking bag that stymies any tracking app....)

It's time to stop thinking of these petite but powerful machines as phones and start protecting them like computers.

The last, and perhaps most important, element of securing your smartphone is smart use—awareness. Hackers have long been able to intercept information over open Wi-Fi networks. Even the strongest protection, WPA2, has exploitable security flaws. So unless you're on a trusted network, don't enter any personal information or check important accounts. That free airport wireless network? You'd be foolish to enter your email, social network or banking information over that connection. You just don't know who's watching. •

Someone stole your smartphone—now what?

1. Find that pen-and-paper list.
2. For all accounts, websites and documents on that phone, change the password immediately—Gmail, Facebook, Dropbox and even your secure work connection. With reverse phone lookups, anyone with five bucks and your cell phone number can find more personal information, from addresses to tax and real estate records.
3. Consider a credit- or fraud-monitoring service. A dollar spent on prevention can save hundreds on a cure.

Don't Turn That Dial

Identity theft aid arrives over the airwaves

We've all had that moment when we're in a tough spot and wish a booming voice would just tell us what to do.

For frustrated identity theft victim Caroline Shafer*, it happened—over the radio.

Shafer had tuned into Ronn Owens' radio show on KGO Newstalk 810 in San Francisco to hear his guest, Identity Theft 911 chairman and founder Adam Levin, tell listeners what to do if their identity were stolen.

Everything Levin recommended Shafer knew from firsthand experience—because she'd already tried it.

"I thought to myself, 'Great, I've done all that, and it didn't work,' " she said. And that's when she picked up the phone.

Shafer told Levin that for more than a year, she'd struggled to correct her credit report after an identity thief used her Social Security number to open bogus accounts, get an apartment and even skip out on a traffic ticket. Despite her efforts—and those of a widely advertised identity theft prevention and recovery service—fraudulent accounts still comprised nearly half her credit history.

Although Shafer didn't have Identity Theft 911's services through her bank or insurance company, Levin took her case anyway.

Levin connected her with veteran fraud resolution specialist Kennetha Gwin. And things began to turn around.

"When I first spoke to Ms. Shafer," Gwin said, "I told her I was here to help her, and I would be with her every step of the way. I wanted her to know that I was going to take much of the pressure and worry away from her."

Gwin crafted a systematic letter-writing and calling campaign, built on affidavits, police reports and credit details supplied by Shafer. By coordinating efforts among individual creditors and the three major credit bureaus, Gwin peeled away the bogus accounts.

She also shut down future fraud by placing an alert on Shafer's credit file, which requires potential creditors to call Shafer before opening a new account. Gwin recommends this free protection to all consumers and encourages everyone to check their credit reports annually at annualcreditreport.com.

"I'm so lucky. Kennetha took charge and did an incredible amount of work. Identity Theft 911 gave me back my life." — *Caroline Shafer*

She also tells identity theft victims to pass along the knowledge they've acquired and help other people protect themselves. "When I send out our tip sheets, I suggest to clients that they share the information with family and friends," she said.

Now, several months later, Shafer is glad she made that phone call. Her credit report finally reflects, again, the responsible person she truly is.

"I'm so lucky," Shafer said. "Kennetha took charge and did an incredible amount of work. Identity Theft 911 gave me back my life." •

** Identifying details have been changed to protect the victim's privacy.*

Hail

No Socials in the Slammer

Social Security numbers will be kept off government checks and away from federal inmates following the recent passage of the Social Security Number Protection Act of 2010. **Sens. Dianne Feinstein (D-Calif.) and Judd Gregg (R-N.H.)** sponsored the bill, which bars federal prisoners on work programs from gaining access to Social Security numbers and prohibits the use of any part of that data from being listed on any check issued by a federal, state or local agency. "Social Security numbers are among Americans' most valuable but vulnerable assets," Feinstein said. "Identity theft is a serious concern for all consumers and we should make every effort to protect personal information." President Obama signed the bill into law Dec. 17. Looks like the only numbers these cons will be seeing are on license plates.

Ukraine's Most Famous Must Face Bad Press

A new law screening public persons from press scrutiny takes privacy protection too far, critics say. Ukraine's most prominent media watchdog claims a new personal data protection law curbs freedom of expression while cloaking itself as a security safeguard. **Natalia Ligachova**, the editor of *Telekrytyka*, says the law's failure to define a public person allows any prominent figure to suppress publication of any information he or she dislikes. She urged newly elected President Viktor Yanukovych to send the law back to the national parliament to safeguard press freedom while preserving personal data security. How long before Italian Prime Minister Silvio Berlusconi sets up house in Ukraine?

FTC's Top Techie Says Web Trackers Should Just Ask

Online marketers should ask customers for information rather than rely on firms that silently compile reports on user behavior, says the new Federal Trade Commission chief technology officer. Princeton University professor **Edward Felten**, the point man for the FTC's efforts to bolster consumer privacy protection—and the man who cracked the music industry's digital copyright protection code—says direct requests from advertisers will be more accurate than tracking web use without telling customers. The agency is mulling a do-not-track provision, similar to curbs on telephone marketers, to make computer user information more secure.

Hiss

U.K. Cop Database Stores the Good, the Bad and the Ugly

Privacy advocates say **local police forces in the United Kingdom** overreach by storing information on people who call to report crimes. About 8 million caller records are stored on at least 22 databases, which are vulnerable to misuse, police watchdogs say. Breach of that data could threaten caller privacy, as well as cast people who report crimes in the same light as criminals because they appear in police records. Shami Chakrabarti, director of privacy advocacy group Liberty, says hanging on to millions of caller records "for decades on end is disproportionate to any legitimate policing goal." Sounds like the Good Samaritan finishes last.

War Games It Ain't

The **Pentagon Federal Credit Union** reported that one of its laptops was hacked and infected with malware that exposed members' personal and financial information—including names, addresses and Social Security, account, credit card and debit card numbers. PenFed hasn't disclosed how many people were involved, but a letter to the New Hampshire attorney general's office said at least 514 New Hampshire residents were affected. Members will get two years of credit protection, PenFed officials said. Good thing the Pentagon isn't in charge of national security. Oh, wait....

Thieves 1; Wayward Spouses 0

Australia's privacy commissioner will investigate reports that data on 4 million **Vodafone** mobile customers was exposed in a massive security breach. Names, addresses, driver's license numbers, credit card details and logins appeared on the Internet, according to media reports. Australian Communications Consumer Action Network head Michael Fraser called it a major breach of the company's privacy obligations and "unbelievably slack security." Vodafone, a London-based mobile communications provider, is reviewing its security procedures and has reset its passwords. There also are reports that suspicious spouses are making use of the info to see what their loved ones have been up to. Seems things aren't looking up for data security—or adulterers—Down Under.

Q&A with Vicki Volkert

Close the door on identity thieves during a move

Question: I'm moving, and I've heard that makes me a target for identity theft. What steps should I take to keep myself safe?

Answer:
You're wise to be aware of the increased risk of identity theft during a move. It's a busy time and everything is in transition, which makes you extra vulnerable.

It's mail in particular that puts you at risk. I bet you get a lot of mail for people who used to live at your address—and if you're getting other people's mail, then someone else can get yours at your old address. This puts valuable personal information—credit card offers, account numbers, Social Security numbers—in the hands of total strangers.

In a move, organization and planning equal security. Here's a good schedule to follow:

Two months before your move: Start a list of all the businesses, organizations and people you'll need to notify of your new address (see box for suggestions). Keep the list handy and add to it every time you remember a new entry.

Start purging your files. Why move old records and risk exposing them in the process? Cross-shred everything you don't need, and, if at all possible, plan on carrying important papers with you instead of sending them with movers.

One month prior: Go to USPS.com or your post office and fill out change of address forms. The postal service will send a confirmation to your old and new addresses.

Take your list and notify everyone on it online or by phone or mail. Include your old and new addresses and the effective date of your move. Take notes on all your correspondence. (You don't want to do this any earlier, or your mail might go to your new address before you're there.)

Moving day: Depending on how far you're moving, take with you your most valuable information, such as financial documents, deeds, checkbooks, medical records and address books. If you're moving across town and the movers will only briefly have access to your things, you can be flexible. But if you're moving to another state or country, you don't know who's going to come across your information. If your move is complicated—maybe you're living in a short-term location until your new house is ready—consider having the post office hold your mail and placing a 90-day alert on your credit file.

After the move: Once you're settled, use your list to keep track of companies mailing to your correct address. Contact anyone who's not and let them know your account may have been compromised.

For a safe move, be cautious and thorough and plan ahead, and your new home will be a cause for celebration, not regret.

Moving notification checklist

- Accountants and attorneys
- Airlines (for frequent flyer accounts)
- Alumni associations
- Banks and credit unions
- Churches and clubs
- Credit bureaus
- Creditors (mortgage holders, credit card companies, etc.)
- DMV
- Employers
- Health care providers
- Investment and brokerage companies
- IRS
- Magazines and newspapers
- Schools (yours and your children's)
- Unions
- Utility companies (including cable and Internet)
- Veterinarians
- Voter registration