

## **Internet Fraud: What it is, how to spot it, and what to do when your client get stung**

by: **Alex T. Roshuk**, Attorney at law  
("Theophan Paine" Second Life [SL] pseudonym)  
© 2008, *All rights reserved.*

**Presenter Introduction:** Alex T. Roshuk is an attorney with a practice in the *State of New York*. He has two law degrees from *McGill University, Faculty of Law*, Montreal, Canada (B.C.L./LL.B., 1997) and has been a lawyer in *New York City* since 1998 advising businesses, individuals and not-for-profit organizations in transactional and litigation related matters. He was the first legal advisor to the *Wikimedia Foundation, Inc. (Wikipedia)* from 2003 to 2005 assisting with the organization's tax exempt application to the IRS, trademark applications, and various copyright related issues.

Prior to becoming a lawyer Mr. Roshuk worked in the entertainment industry as a film editor, radio announcer, television producer and director and as an administrator and/or director of numerous not-for-profit media arts organizations in the United States and Canada. He studied electrical engineering at *Princeton University* in the 1970s. He currently lives and works in Park Slope, Brooklyn, NY, USA. He is an elected member of the *SL Bar Association Executive Committee* (term ending Summer 2008).

**Lecture Introduction:** The rise of the internet has been a boon to scammers, confidence artists, swindlers, grifters and psychopaths. The ease of communication over the internet, and the metaverse of digital simulations like Second Life has allowed these professional criminals the opportunity to develop a new environment in which to peddle their schemes to unsuspecting members of the public. This lecture will introduce you to the types of fraud, how to spot it before you or your clients become victims and what steps can be taken if you discover that you or your clients are victim of these types of criminal activity which may result in serious damages.

### **Course Outline:**

- I. ***Internet fraud: What is it?***
- II. ***How to spot internet fraud***
- III. ***What to do when you or your client are victimized***
- IV. ***Victim of an allegation of "click fraud" but innocent?***
- V. ***Annotated bibliography, references and useful links***

## 1. ***Internet Fraud: What is It?***

**INTRODUCTION:** The basic types of internet fraud and some of the more common schemes. The creation of the false personality, false company, false company relationship is often done through the internet with a gullible individual that is presented credentials, scanned documents, False addresses, unusual proposition. Sometimes the more sophisticated internet fraudsters use real life situations that may contain elements of reality so as to confuse the “mark” or victim of the fraud and the best criminals try to reduce their fraud to civil fraud so that it is hard for

## 2. ***How to Spot Internet Fraud***

**INTRODUCTION:** The false personality, the mail drop, various money wire schemes, The person contacting you is far away, in another country and the only way you can communicate with them is through the internet, a chat program or Skype or when they call you it is through some untraceable and unreturnable telephone call.

When efforts to verify the identity of the persons involved are futile except through documentation that is not really acceptable identification it is likely that some kind of scam is being set up, it may be an attempt to make the person conducting the scam “judgment proof” so that the victim may find it very hard to seek redress. A commercial con artist may promise all kinds of results, but the proof of these results is often charts that cannot really be interpreted.

Following are a few examples of the various “cons” or confidence games that are “played” on the internet or through it. The nomenclature of ***Big Cons*** and ***Short Cons*** comes from How to Become a Professional Con Artist, by retired P.O. Dennis M. Marlock, (Paladin Press, Bolder CO, 2001). *Short Cons* occur quickly and involve a short term interaction with the “mark” or victim and *Big Cons* involve ongoing long-term (sometimes months or years) interaction with the victim.

## **SHORT CONS:**

*The Short Order Scam:* Providing used clothing to out of town customers who make orders over the internet. The orders are only partially completed (90 or 95%) as the customer will have a difficult time suing when they are thousands of miles away and possibly cannot come to the United States because a visa is impossible to obtain and the cost of litigation outweigh the losses people just give up. What can you do? Sue in a small claims Court through the mail?

*eBay or Auction Scams:* Selling an artwork on eBay that is a mere copy of an original work without first obtaining the *Certificate of Authenticity* or another third party verification that the work is an original. Or selling an item but never actually shipping it after asking for payment by “wire” “bank check” or *Western Union*. N.B. companies such as eBay are protected by Sec. 230 of the *Digital Millennium Copyright Act*, a US Federal Statute.

*Phishing and spoofing emails:* This is a common occurrence, we receive an email from a bank asking for account verification, or eBay or Paypal the address looks legitimate, however there is a different address hidden in the link that brings you to a “spoof” website that looks almost identical to the legitimate website log-in page. At that point you enter your log-in information and the scammers then take control of your real account. These may also involve trying to get your bank account information by posing as a potential client that wishes to send a payment from a country such as Switzerland (a country rampant with money laundering problems) where they can wire you money if you give them your bank account and routing information. Note that this information is all that is required to make copies of your checks which are then used in various fraudulent check schemes, with your account information and address on them!).

## **BIG CONS:**

*Romance Fraud:* a criminal gang in the former Soviet Union establishes a “boiler room” operation of 5-6 individuals who send out emails to unsuspecting men in Western Europe and the United States through various “free” dating websites. After a short email correspondence with a man “she” (really one of the fellows in the boiler room) begins to “tell” him of her love for him. She tells him that she can come to visit him if he contacts a certain “tourist” company near her home town (she often lives in a small village or town and she cannot call and only has access to the internet. She tells you that you can “purchase” her ticket through this company. However the company does not take credit cards and the money must either be wired to a bank account or it must be sent via Western Union to some third party in a remote city in Russia, both services that provide no security or ability to reverse the transaction once it has gone through. One case was actually done by an American man with a Russian girl friend that used pictures of her friends in Russia. She would call the man and ask him to wire money to Russia (to her relatives) for “visa and airfare” to the US to visit the man, this was 40-year-old Robert McCoy from San Diego, California who was order to repay over \$700,000 to approximately 250 American men that he and his Russian wife scammed.

*The “Nigerian” Advance Fee Fraud:* Your client is contacted by email being informed of a large “inheritance” or amount of money held in trust in some bank in a central African country and promised a large percentage of the money in exchange for helping them. They need your client’s help in getting the money out of the country. At the beginning the help is just using their name and address as the beneficiary, but eventually they convince your client to send money to pay for certain fees (these are the advance fees) that are needed to get the money out of the country. Usually the person writing to your client says they are not in Africa but the emails are, in fact, coming from Nigeria. As the article from the May 15, 2006 issue of *The New Yorker* magazine shows (see bibliography) this can be very dangerous and it is not just the uneducated or uninformed that fall prey to these schemes.

*Collection Agent Commissions:* Your client is contacted by a Chinese company that exports vast quantities of goods to North America. The short email is from the President of the company. They are searching for a NA agent and can send your client outstanding invoices; your client has to contact the companies here in North America who will send your client payments to be deposited in your clients bank account (making your client an accomplice to money laundering) and send a payment of cash through “Western Union” (because this is the only way they can get the money according to them) to a third country overseas.

*International Visa and Business Opportunity Web Sites:* Your client is asked to become a “member” of an exclusive service that can help you develop an “off-shore” business. Your client is offered the opportunity to work with one of the “Advisors” to help your client to obtain a visa or even “economic citizenship” in an offshore country, your client is given references (all fake websites, with phone numbers and mail drop addresses in multiple countries leading back to the same criminal gang) and this “Advisor” promises to have an exclusive “off-shore” account opened for your client at the “United Nations” branch of one of the world’s largest banks, all through the internet. After your client shares personal information with the scammers they contact your client’s relatives in your client’s name and convince them to make deposits in accounts allegedly owned by your client, however the account is not really in your client’s name and the money quickly disappears out of that account into another account in another bank in another country.

*Re-shipping Services:* Another variation on the ten percent commission scam. Here your client’s address is used as the shipment address for stolen credit card orders and they are paid a commission plus expenses for repackaging the merchandise and shipping outside the United States. Your client is asked to pay for shipping and then to be reimbursed weekly. Often the reimbursement checks are bad and you are left having made large disbursements (a variation on work at home scams) or the monies received are also being laundered when your client is asked to make purchases with these funds. Your client may be guilty of a criminal activity because they have handled stolen goods. It is not a defence that they were unaware of the fact they were handling stolen goods.

## **STEPS TO TAKE BEFORE YOU OR YOUR CLIENTS ARE SCAMMED:**

**Track the emails that you send.** If someone says they are writing you from China with a Hong Kong email but the email is actually coming from Canada you can use a tracking service to discover the origin of the email. Email tracking services are available for approximately \$5.00 per month such as readnotify.com and are well worth it (also can be used to prove delivery of time sensitive documents and can verify sending of documents) or “HIPAA compliant” email systems (that allow you to send encrypted emails through an online server such as certifiedmail.com)

**Obtain verifiable third party documentation.** Ask for copies of corporate documents that have a proper “apostille” or are certified by an authority that can verify identity (usually the best is to ask the person to go to your country’s Embassy and have a copy of their passport photo page verified for identification purposes). Find someone in that country that is reputable (may be difficult in countries that are very corrupt, even high level bar association officers may be willing to accept a bribe from a corrupt individual) to verify identity, corporate status, etc.

**Use Search Engines to do “reverse” analysis of the information you are sent.** Stripping off the name and address information and searching using addresses, phone numbers, short phrases (particularly useful in romance scam cases as large databases of scammers and their letters are published online) can link you to a site that can show that the address you have been given is a mail drop, or private residence (when it is touted as a “corporate headquarters”).

**Never forget standard due-diligence searches.** Checking a local *Chamber of Commerce* or making inquiries through a local investigator can uncover a scam relatively easy. Examples are addresses of elderly individuals that are used as “drops” for businesses or someone who does not want their real address given to the victim, linking someone to some kind of local criminal gang. N.B. that sometimes investigators can be scam artists themselves. If the business requires a license, check the licensing body, do not rely upon an online copy of the license (often forgeries). Find someone who speaks the native language if dealing with a web site purported to be in a foreign country.

**Travel to that country and verify all the information there.** *NOTE THIS CAN BE DANGEROUS!* If someone sends you a picture of their office, you may discover that it is an “instant office” location once you arrive there, or even a mail drop. These kinds of “fact finding” trips can be dangerous if the person going to investigate is not very familiar with the local language and customs and does not have the savvy to realize that he or she is being scammed.

### 3. *What to do when you or your client are victimized*

#### **INTRODUCTION:**

The sad fact is that before reporting a case to the authorities you must determine if your client has committed a crime by participating in the scheme. Sometimes 10% “commission” schemes are just money laundering and the transactions appear to go through your clients bank or trust account without incident. However, often these transactions are efforts to launder money through a vast international network that uses your client’s bank account in an unsuspecting way and your client may, in fact, be guilty of money laundering. In such case it would be imprudent to report it to the authorities unless you can obtain some kind of immunity for your client beforehand and can protect your client from any disclosure that might be contrary to the attorney-client privilege.

If you have determined that your client is not in violation of any jurisdictional law (including RICO statutes and other related economic crime laws) and can report it, such as the case where your client was just the victim of a theft, there are a variety of agencies where the incident may be reported. However, many fraudsters are able to create the semblance of a legitimate business around their operations and if they are sophisticated they will tell their bankers, the police and anyone else who asks that you are just a disgruntled customer who has a gripe with them because they are not satisfied with your services and that any dispute may be resolved through the Courts in a proper legal manner. As well, many individuals are scared to report such cases as they feel that they somehow acted criminally themselves. However, usually the client (or even you) did nothing wrong other than participate in an elaborate hoax. No one is going to prosecute you or your client from trying to obtain a some of money from a foreign bank for its depositor because he was forced to leave the country due to insurrection.

What to do when all else falls: sue, sue, sue! It is possible to sue someone in another country and it is not that complex a procedure. With the documentation that you can obtain through the internet often there is sufficient long-arm jurisdiction over the fraudster. Your judgment may be expensive to procure. However they may be times when filing a case can result in a positive outcome. I had one case that involved sale of a flat screen television. The seller was here in Brooklyn and purchaser was far away. He purchased a bank check payable to the seller who didn’t send him the goods. The purchaser obtained the eBay account information that was in the name of an older woman (though the purchaser dealt with a younger man). Turns out the older woman was the mother of the scam artist and after she was sued she was able to get her son to reimburse the lost monies.

Filing a case in Federal Court against a foreign national may be the only redress. Again while it may not seem possible to obtain a result (recovery) for your client, filing a simple complaint may be all that is necessary to scare the scam artists (if they are not from

a country where criminal gangs operate with the assistance of law enforcement). It is possible in many countries to serve such complaints by *Registered Mail* or if it is not allowed most countries are signatories to the *Hague Convention on Service Abroad* and sending a request (often free) to the foreign authorities. To obtain testimony or discovery in foreign countries it is necessary to do this through "Letters Rogatory" that can be done through the U.S. State Department.

## **USING RICO**

A powerful federal statute known as the *Racketeer Influenced and Corrupt Organizations Act* (18 U.S.C. §§1961-68) provides a powerful, albeit complex tool to obtain damages and legal fees against scam artists. While a complete analysis of this law is beyond the scope of this talk this law that requires several elements to be proven.

To state a claim, a plaintiff must allege four elements: (1) conduct (2) of an enterprise (3) through a pattern (4) of racketeering activity. Each element above also requires additional analysis: an "enterprise" is must have association and control; the "pattern" requires a showing of "continuity"-continuous and related behavior that amounts to, or poses a threat of, continued criminal violations; and "racketeering activity" involves the violation of designated federal laws (often referred to as the "predicate offense"). The plaintiff must allege that he or she was injured in his business or property "by reason of" a violation of substantive provisions.

While bringing a RICO claim is complex it has many benefits including treble damages and recovery for attorney fees. Crafting a complaint that can survive motion practice may be difficult, however many scam artists may not even contest a claim and while the complaint must be sufficient to get a default judgment, the increased amount of the judgment (and using RICO to "pierce the corporate veil") may help to obtain information or even assets under the control of the racketeering organization.

## **DEALING WITH A "JUDGMENT PROOF" DEFENDANT**

It is always important to remember that when dealing with scam artists, they have often made themselves somewhat "judgment proof" and unless you can find mistakes they have made. However since most scammers don't hire defense counsel it may be possible to uncover assets or information in the process of obtaining judgment enforcement as many scammers using internet merchant services, bank services, Western Union services or other corporate services where all activity is well documented and can be linked back to credit card numbers and bank accounts. Monies that flow in and out of international banks by wires often go through "correspondent" banks that are located in New York or London and it may be possible to obtain jurisdiction of these courts if it can be shown that the funds passed through these jurisdictions. Even sending subpoenas through the mail may result in alerting authorities. In one case I sent a copy of a discovery subpoena to a defendant to a mail drop address and it was intercepted by national police agency investigating a group that was posing as a service that needed local regulation which helped me confirm the identity of those involved for local civil proceedings.

#### **4. Pre-Action Discovery Procedures: victim of an allegation of “click fraud” but innocent?**

Recently individuals and companies who are using services such as *Google’s* AdWords to “monetize” their web site and many new websites are accused of “click fraud”. While it seems impossible to successfully sue companies such as *Google* or *Yahoo* due to user agreements that require binding arbitration, it is possible to do discovery against these companies to obtain valuable information regarding these allegations of click fraud as regards third parties, if in fact, the click fraud is not originating from your client. Often what *Google* calls “click fraud” may be someone attempting to block your client’s site from successfully monetizing their site(s) and such tortious acts should be clearly actionable in most jurisdictions.

Many jurisdictions have mechanisms in their civil procedure laws that allow for filing “pre-action” discovery to preserve evidence. In New York City these can even be filed in a lower court (*Civil Court of the City of New York*) that is quick and cost effective. They allow for the issuance of subpoenas, court ordered depositions (EBTs) and other discovery devices such as interstate (domestic and international) *Letters Rogatory* (which may require a long time to complete).

While *Google* and other online advertisers will not give you any information regarding the exact nature of the alleged “click fraud” since you are alleging that the third party acted to create the impression of click fraud the Court has the jurisdiction to order the advertising provider to turn over the necessary information. N.B. that when you serve a subpoena on *Google* they ask for a complex confidentiality agreement before they are willing to turn over information to you because they believe that you will learn how their vast empire works and will use it to create your own billion dollar enterprise.

## 5. **Annotated bibliography, references and useful links**

### **Books and websites about fraud, confidence schemes and other cheats:**

Marlock, Dennis M., *How to Become a Professional Con Artist* (Paladin Press, Boulder CO, 2001)

Written by a former police officer, provides all the information that Con Artists use and can be useful in spotting various confidence schemes.

Maurer, David W., *The Big Con: The Story of A Confidence Man* ( Anchor Books, Random House, NY, 1999)

A famous journalistic account of the Big Con written by a Professor of Linguistics which inspired George Roy Hill's film, *The Sting* (1976).

Zukoff, Mitchell, "The Perfect Mark: How a Massachusetts psychotherapist fell for a Nigerian e-mail scam", (New Yorker magazine, May 15, 2006) [http://www.newyorker.com/archive/2006/05/15/060515fa\\_fact](http://www.newyorker.com/archive/2006/05/15/060515fa_fact)

Shows how dangerous falling for an online scam can be and some of the consequences and how the victims are often very intelligent well educated individuals.

<http://career-advice.monster.com/job-search-essentials/Money-Laundering-and-Reshipping-Sca/home.aspx>

Provides useful information about online "employment" scams such as work at home and various money laundering schemes.

[http://travel.state.gov/travel/cis\\_pa\\_tw/financial\\_scams/financial\\_scams\\_3155.html](http://travel.state.gov/travel/cis_pa_tw/financial_scams/financial_scams_3155.html)

U.S. *Department of State* web page that provides useful information about financial scams usually involving the internet in some aspect.

[Http://www.ripoffreport.com](http://www.ripoffreport.com) :

A private website that allows individuals to list companies that have "ripped off" individuals or business. An example of useful place to do due diligence on the internet to find businesses or individuals that engage in fraudulent practices.

<http://www.russian-detective.com/scams.htm>

Another private website that specializes in information about Russian romance scam web sites and criminals.

### **International Law Jurisdictional issues:**

*Hague Conference on Private International Law* website: [http://www.hcch.net/index\\_en.php](http://www.hcch.net/index_en.php)

This is a valuable website that has the text of many PIL treaties or conventions and current lists of the signatory states and the local or municipal “authorities” in each state that are responsible for providing services under each Convention.

*US Department of State*, Judicial Assistance web pages: [http://travel.state.gov/law/info/judicial/judicial\\_702.html](http://travel.state.gov/law/info/judicial/judicial_702.html)

This directory to a series of pages at the *US Department of State* provides valuable information (including applicable US federal case law and reference to various treatises) that deal with such relevant issues as “Apostilles” and document authentication, *Service of Process* abroad under the rules of comity or the *Hague Convention* and problems relating to the Enforcement of U.S. Judgments abroad.

*Martindale-Hubell Law Digest*, Vol 2., International: State laws and international conventions and treaties (2008, updated annually)

This is a valuable publication by *Martindale-Hubell* (that also produces an international directory of lawyers) that provides digest information on various international state laws and the texts of treaties and the *Hague Conventions* such as the *Service Convention*.

*United States Marshall's Service*: [http://www.usmarshals.gov/process/foreign\\_process.htm](http://www.usmarshals.gov/process/foreign_process.htm)

Provides information about serving defendants in the United States from foreign countries and also a link to the USM-94 form “Request for Service Abroad of Judicial or Extrajudicial Documents” which is required when sending a service request overseas to a signatory state “authority” (you may also use translated versions of this form found at the *Hague Conference* web site). Note that some countries require that the papers be translated into the official language of the receiving state if compulsory service is requested.

### **Miscellaneous**

The Internet Archive: <http://www.archive.org>

An extremely valuable web site that can provide historical information on a web site. This may provide useful information as the owners of the website may have previously published information and now removed it, changed company names, changed addresses. Few people realize that such a historical archive exists and that this information is readily available for free.

***Books about Civil RICO and laws that may protect your client:***

Newman, Stephen A., and Imholz, Elizabeth M., *Caveat Venditor: A Manual for Consumer Representation in New York* (Julius Blumberg, NY, 1994)

Written by a NYU Law Professor and a legal aid lawyer this book provides the practitioner with a panoply of suggestions regarding a variety of laws and legal strategies that can be used in New York State (and to some degree in federal courts) when “consumers” are victimized. Even though written before the advent of the internet many of the suggestions are applicable to website or email scams.

Abrams, Douglas E., *The Law of Civil RICO* (Little Brown and Co., Boston, 1991)

A law professor’s introduction to the “creative” use of the federal and 18 U.S.C. §§1961-68 RICO statutes and various “Little RICO” state statutes. Provides basic and useful introduction to the RICO laws for any practitioner contemplating bringing a RICO action in State or Federal Court in the United States(not updated).

Smith, David B. And Reed, Terrance G., *Civil RICO* (Matthew Bender, 1987-, updated)

A standard practitioner’s treatise on RICO.

Joseph, Gregory P., *Civil RICO: A Definitive Guide* (American Bar Association, Section of Litigation, Chicago Ill, 1992)

Some of this book is available for preview on *Google Books*.