World Privacy Forum Report on Online Job Scams, Pt. I

A Year in the Life of an Online Job Scam: A Longitudinal Study

Pam Dixon, Principal Investigator (*)

www.worldprivacyforum.org

I. Introduction

Job scams are as old as jobs themselves. In past years, con artists would put a bad job ad up, fool a job seeker into giving up their money, and then physically move on to a new city. Now bad job ads have moved onto the Internet, with devastating consequences. The very things that make the Internet so effective for job seekers -- speed, convenience, and a nationwide job search from a computer screen -- are the same things that make it effective for fraudulent activity. Job seekers and job sites have unfortunately been targeted with sophisticated triangulation scams that move rapidly and seamlessly through a selection of job sites from coast to coast in a matter of days.

In this report, The World Privacy Forum is publishing the first documentation of the detailed path of an online job scam as it worked its way across multiple job sites over the course of a year. The documentation of this scam, its evolution, and its devastating effects on the victims it has left behind provides the first clear longitudinal view of the scope, patterns, and severity of the online job fraud problem.

The particular scam documented in this report is not a "mom and pop" job. It is larger and more sophisticated than it appears on the surface. The footprints of this scam are documented and presented in the "Evolution of a Job Scam" timeline in Section IV. This scam is dangerous and has been perversely effective in defrauding its victims.

One of its victims got fired for simply being duped by the scam. Another person's bank account numbers were stolen and used. As of

June 2, 2004, the World Privacy Forum has confirmed that there is a worst-case scenario connected with this scam: a victim of this scam has been arrested, indicted, and now faces trial for criminal charges directly resulting from being apparently tricked by this bad job ad into forwarding money that had been stolen. (For a description of how the scam works, and why this victim was charged with a crime, see the "Payment Transfer" discussion in Section II.)

It is important to note that an indictment of a job fraud victim represents a sea change in the "grace period" job scam victims had been enjoying until now. Just as identity theft victims had to fight a hard battle to help people understand their plight, the same challenges now face job seekers victimized by slick, organized job scams.

The World Privacy Forum views this change in approach to victims as a tipping point for the job search industry. The stakes for correcting the job fraud problem have become very high, and this complex issue must now be addressed in the strongest possible manner that provides the most effective proactive protection to job seekers.

But getting rid of job fraud will not be simple or easy. Job fraud is a stubbornly complex issue, and it is deeply and subtly intertwined with challenging data privacy issues. It is also an issue that extends beyond online job sites to the entire job search sector.

For at least the past 11 or 12 years, the Net -- more specifically the Web -- has been home to hundreds of job sites and millions of job ads. Internet job distributor eQuest estimates that in 2002, it sent out over 24 million job ads to an array of approximately a thousand job sites (1). Those ads represent many good opportunities for job searching.

The virtues of an Internet job search, in the hands of criminals, have become a nightmare for both the job seekers and the job sites alike. While in past years con artists just stole money from a handful of job seekers city-by-city, now computer con artists are stealing money, identities, bank account numbers, and SSNs across the nation with relative ease. Job scams are so effective in the online medium that it is nearly impossible to catch up with the criminals until after the damage is done.

Job sites, for their part, do not simply throw open their doors to let theives steal resumes or to post fake jobs. In fact, many job sites have

been in the process of seeking strong solutions to the growing problem of job fraud for well over a year or more (2). It should be noted that not all job sites have a history of fraud complaints, but many do.

Since November 2003, the World Privacy Forum has been conducting a study of job site scams and related resume database privacy issues. Researchers have been working to quantify the overall percentage of job scams on job sites, figure out how they operate, discover their patterns, and find ways of circumventing the scams. The point is to protect current job seekers as well as to create a research-based understanding of the problem the job search industry faces.

Part I of the study involves a longitudinal study of a single scam to discover long-term patterns of scam evolution and activity. Part II of the study focuses on quantifying the amount and type of job scam activity.

The preliminary findings of Pt. I of this report are both positive and negative. There has been improvement, but more needs to be done. The goal of this report is to help give consumers and organizations the information they need to begin to combat this complex, stubborn problem before there are any more victims.

As part of this report, the World Privacy Forum asked the largest job sites to respond officially with details of what they are doing right now to combat job fraud. This report contains their detailed responses in Section V, and it includes a timeline detailing each documented incidence of the scam described in this report (Section IV).

The World Privacy Forum made a good faith effort prior to the publication of this report to notify each site where researchers found and documented the fraudulent jobs.

A. Positive Findings Regarding Job Site Response to Job Fraud

* The largest job sites have already instituted mechanisms to allow consumers to officially complain about job fraud by email or telephone. These mechanisms need improvement, for example, on one site, a fraudulent job was taken down many hours after notification

that it was a fraud. But at least mechanisms are in place to be improved upon.

* Many sites have instituted consumer education campaigns and consumer protection tips on their respective sites. This is a positive and proactive step, particularly when the tips are on each job ad.
* Sites are slowly finding effective ways of dealing with fraud through experience. Some smaller job sites have resorted to checking every job ad before the ads get posted. This is a labor-intensive process, but it is effective for smaller sites. Other job sites, such as Hotjobs.com, do not accept certain categories of jobs whatsoever, those for example being job categories that have had high fraud reports in the past. This deletion of problematic job categories is a positive step for consumer protection.
* Preliminary results indicate that job scams can be thwarted when consumers can readily find the names of the fraudulent companies the ads have appeared under. After the World Privacy Forum and the Privacy Rights Clearinghouse published a consumer alert on a job scam in December, the organizations received numerous phone calls and questions asking about the companies mentioned in the alert. In some instances, jobseekers were spared from being victimized by the fraud because they found the alert before they handed over a contract with bank account numbers and other personal details.

B. Negative Findings Regarding the Job Fraud Problem

* Job fraud online is a substantial consumer issue. Although researchers cannot fully quantify the percentages of the overall numbers of scams posted yet, the detailed timeline in this report is certainly an indication of the scope and breadth of how broadly just one job scam can reach.
* Reposting of known fraudulent jobs is a substantial problem at some sites. Some sites do not have effective methods in place yet to avoid reposting identical fraudulent job ads even after they have been taken down one or more times.
* Even the largest job sites, if working alone, would likely not be able to see the full picture of how widespread a particular fraud is or how it interconnects with other job postings. Because of their natural isolation from each other due to competition, job sites have been left with a nearly impossible task of figuring out how a fraud ring is operating by looking at the individual job ads at their site. It would be a far more effective strategy for job sites to work together in order to

obtain a comprehensive view of fraud so that all iterations of a scam can be shut down.

* A technical finding is that RSS (Real Simple Syndication) job feeds will need to be tweaked for the job search environment if RSS continues to grow in popularity. (See Recommendations, Section I. c).

* Preliminary findings indicate that banks have a role in preventing victimization in job fraud scams, but preliminary indications also indicate that the banks the victims of the scam this report documents have been caught unawares on this issue. Over the course of the eight months the World Privacy Forum has been closely tracking this issue, many if not most of the job scam victims reported to the World Privacy Forum that they called their banks and spoke to bank officials before proceeding with the scam, and were reassured by bank tellers and others that the scam was legal and fine. In some cases, bank employees reported victims to the police.

* Job fraud victims have not found good avenues of support as they search for information and help. They often do not know who to call, because they do not fall into the category of pure identity theft victims and they are often not sure of what has happened to them until after the fact. Sometimes, a victim's first indication of a problem is that they are arrested after they have applied to a job, only later to find out was a fake. Much more needs to be done specifically for victims of job fraud.

C. Recommendations

* Job seekers need a mechanism that will allow them to gauge the trustworthiness and effectiveness of a job site's protection against bad job ads. Currently, this does not exist. There is almost no transparency for consumers trying to make this kind of judgment.

* Job sites need to begin to work together to create workable and creative solutions to combat job fraud on a macro scale. Job sites working alone will be at a disadvantage, because the con artists have a pronounced pattern of working on multiple sites at once using different job ad names.

* The entire job distribution infrastructure needs to be involved in a solution to the job fraud problem. Just cleaning up job sites is not an effective strategy. Job distributors and their suppliers will need to be in the conversation for there to be any real and substantive change.

* Consumers must now be the focus of national education campaigns by job sites large and small, consumer groups, banks, and

companies such as Western Union, PayPal and eBay. Now that victims are being charged with crimes, this is no longer optional.

* Many mid size to small job sites do not have the resources to effectively combat slick job fraud rings. This is a long-term issue that can be addressed at least in part by not allowing automated job postings to go up prior to the jobs being reviewed by a person.
* The goal is to never post any job scams. But given that some bad jobs will likely slip through, a fair fall-back position is to never repost a known fraudulent job. It should be an industry standard that this should never happen at any site.
* Banks must educate personnel about job fraud and how it victimizes people. Instead of turning victims asking questions over to law enforcement, victims should be given useful, accurate information about job fraud and scams before they take any actions that would hurt themselves or others.
* Job fraud schemes are dense and are nearly impossible for victims to figure out in enough time. Simple, easy to remember, and effective tips that get at the heart of preventing consumer harm need to be agreed upon by the job search industry and consumer groups, and all parties need to work hard to get this message out to all job seekers or potential future job seekers.
* If RSS -- a technology that aggregates Web site content and allows people to read it offline -- continues to grow in popularity, job sites will need to think about their RSS delivery and address the fact that job seekers still need to see the job fraud information they would ordinarily see on the Web site. This can be managed fairly easily. For example, CareerBuilder puts job fraud consumer protection tips on every job ad. Their RSS job feeds deliver only headlines and minimal information, so job seekers need to go to the site to see the rest of the job. This is positive, because the job seeker will also have access to the fraud prevention tips. Having consumer protection tips on every job ad is a good idea anyhow, but it will be even more important in the RSS environment where job seekers may not have seen much contextual site material about job fraud.

II. Payment Transfer Scams and How They Operate

Payment transfer scams begin with a con artist that pretends to be an employer. The con artist uses a job ad to lure in an unsuspecting job seeker, or they may use information from a resume they have found. The con artists can be quite convincing, and may even steal company names and corporate logos to convince victims that they are

legitimate. After the con artist has won the job seeker's trust, the con artist tricks the job seeker into giving up bank account numbers. The reasons given for this can be clever. One common reason the con artists give out is to say they only deliver paychecks by "direct deposit."

The "job" a job seeker will be asked to do involves forwarding or wiring money from a personal bank account, a PayPal account, or from a Western Union office to another account or person. The other account or person is often overseas. The job seeker is instructed to keep a small percentage of the money as their payment. Sometimes the payment for making the money transfer is as low as $15, sometimes it is as high as several hundred or several thousand dollars. Almost always, the money the victims are transferring is stolen, and therefore, the victims are committing theft. Usually, this kind of scam involves at least two or three victims.

The amounts tranferred in this kind of scam are usually just under $10,000. In Appendix A, there is a good example of this kind of request in an email from the scam artists to a victim. The instructions are to wire $9,600 and keep $480. Transfers in amounts under $10,000 are subject to less scrutiny from banks than amounts over $10,000.

There are many variations of payment scams, but following are the basics of how a payment forwarding scam works:

1. The con artist poses as an employer, sometimes very convincingly. Often, names of real companies are used, and real corporate logos may be stolen from Web sites to make the scam look convincing. The con artist gains access to a job site or job distribution network, and they post multiple fraudulent ads. Con artists may also illicitly gain access to resume information.
2. Multiple victims are recruited through the online job advertisements. The job ads are typically for an accountant or finance manager.
3. After the victim sends the fake employer a resume, the fake employer contacts the victim and goes through a convincing interview process with them. Victims say that this process is extremely credible. The con artist eventually over time lures the victim to give up their bank account number and other personal details.
4. After victims are asked to give their bank account numbers for direct deposit of paychecks.

5. The bank account numbers of some of the victims may be used access their accounts and steal money.
6. The stolen money is used to rapidly purchase goods, often from online sites.
7. A last victim is chosen. This last victim is wired the stolen money from the first set of victims and told it is their (the last victim's) paycheck or a similar excuse. They are told to keep a percentage of the money and transfer the rest to a new account that the con artist gives them. The transfer may take place at a bank, or often, in person at Western Union, or via a PayPal account.
8. The moment the last victim transfers the money, they have unwittingly committed theft because they have transferred and taken stolen money. These victims are further victimized if they are then arrested for theft, which is a real possibility.

Again, many variants of this scam exist. One variant is related to money laundering of stolen credit card numbers instead of stolen bank account numbers. Victims will be told they are processing payments for "domestic sales" of an overseas company, often located in Europe or China. The victim gets deposits into their bank account or a PayPal account, then they are told to forward the money, usually in person, at Western Union. Like in the first variant, the moment the victim transfers the money from the stolen credit cards, they have committed a crime.

The World Privacy Forum has spoken to numerous victims of payment transfer scams, and have found that a good con artist can ensnare even the most knowledgeable financial professionals in these scams before becoming aware of any problems. The key is that even the most reasonable person, given a lack of expertise in computer crime, will typically not understand the complexity of the crime and is typically not equipped with enough information to walk away from the scam in time. (3) The victims of this scam that transfer the money can no longer count on forgiveness.

Note: Another type of scam closely related to payment forwarding scams are the "Postal Forwarding" scams. In this scam, stolen money is used to purchase goods. Those goods are sent to a victim who believes he or she has gotten a job as a shipping or receiving clerk. The victim then forwards the stolen merchandise to an address, usually overseas. The US Postal Inspector General has detailed

information about Postal Forwarding scams available at its Web site:<http://www.usps.com/websites/depart/inspect/ >.

III. Background of the UMAB Payment Forwarding Scam

The scam tracked in this report is a payment forwarding scam. Researchers have given this scam the name "UMAB," which is an acronym of the major company names it has gone under. (See next paragraph for a listing of the names.) The operators of this scam request victims to deposit money into personal bank accounts, and then transfer money from those accounts to three different contacts overseas. The World Privacy Forum has been able to trace this scam from September of 2003 to the current date, July 7, 2004. As of this date, the scam is still active.

The UMAB job ads were posted under various names -- names that have been tied to the scam so far are Unk Electronics, Macrocommerce Intersales, Nanjing Panada*, Antares Electronics, Inc.*, BestElectronics, and Omega, Inc. While researchers cannot be 100 percent certain that the job ads are all part of one scam ring, the likelihood is very strong. Researchers used various methods to tie the ads together (See Methodology, Section X). One of the most reliable ways of confirming that a company is part of the UMAB scam has been for researchers to apply for the jobs and to receive the employment contract, which has unique errors in it. (See Appendix A for examples of email exchanges and employment contracts.)

While the company names change, the posting pattern and the job ads remain largely the same or similar. In some cases, the phone numbers of the different companies match. For example, many Macrocommerce Intersales job ads used a phone number that was an exact match of the Unk Electronics job ads. In other cases, a new company name will be used with a slightly modified job ad. But the actual employment contract for that ad is the same for all the versions of the scam (except for contact details, which consistently change.)

The UMAB scam reveals sophisticated posting patterns that maximize finding new victims without ever overlapping cities or dates where the job appears. A typical pattern for the UMAB scam is that the con artists will test a new company name in a job ad posted to one or two cities on one job site. After a few days or weeks, the ad is launched in more cities, usually four or so at a time, and on a different job site.

After the con artists have a job ad up and running in several areas of the country, the con artists will try out a new company name in a different area of the country. The con artists keep repeating this process of posting job ads on different sites for different part of the county. As the scam evolves, the con artists develop favorite cities and job sites for job postings. The pattern becomes distinct.

The scammers' pattern is devised to keep job sites from being able to figure out that a national scam is in operation. Unless the job sites are actively searching for all incidents of a job ad and actively applying for jobs at all the incidents of the fraudulent job ads, it would be nearly impossible for an individual job site to figure out how a job scam was evolving.

For example, one of the ways researchers tracked the scam is by doing exhaustive searches through a group of job sites and 15 different or more search engines on the patterns of word combinations used in the actual job ad itself. It is unlikely that a job site will have personnel dedicated to this kind of work full-time. But this and more is what it would take for sites to fully piece together a scam's operation.

Approximately 23 job search sites have posted the UMAB scam. Some sites only posted the scam one time. Other sites to date have posted the exact same ad with the same company name multiple times. A challenge all of the job sites face is that company names for the job ads change regularly, which can make it difficult for job sites to catch new iterations of the scam. Tracking by IP address and credit card number can help, but not if the job comes from a trusted job distributor or from within another part of the job distribution infrastructure.

Job sites and other sites confirmed as posting one or more variants of the UMAB job ads are:

* AOL.com career center via CareerBuilder
* Aftercollege.com
* Atlantajob.com
* Australiajobsite.com
* Canadajobsite.com
* CareerBuilder.com
* CareerMag.com
* CareerSpan.com

* Chicago Tribune Online (Via CareerBuilder)
* CollegeGrad.com (College Grad Job Hunter)
* CollegeRecruiter.net
* Dallasjobsite.com
* jobs.pearlhaven.com
* JobSpider.com
* Losangelesjobbank.com
* Lookingforwork.com
* Monster.com
* MSN.com career center cia CareerBuilder
* PickaJob.com
* PreferredJobs.com
* RetiredBrains.com
* Tutorgig.com
* WithinMiles.com
* "4jobs.com" network; Baltimore.4jobs.com, etc.

Some of these job sites are job networks, or related sites that share postings, which made the actual number of Web sites posting the jobs closer to 100. The United States, Australia, and Canada were the primary countries targeted. This scam also appeared on sites in Germany and throughout southeast Asia.

A. Other Findings related to the UMAB Scam

* While the Internet is a global medium, in this scam, certain cities and regions have been strongly targeted. The states of Florida, Texas, and Washington are strong general targets. Sacramento, Houston, Seattle, Miami, and other cities are among the strongly targeted cities. (See Timeline in Section IV for the detailed posting history.)
* The UMAB scam began as early as September, 2003 and is still operating as of July 7, 2004.
* The UMAB scam appears to be run by an organization based overseas.
* The scam is of the "payment forwarding" type and is typically triangulated, which means that it uses multiple victims to obscure and hide the actual details of the scam.
* Victims who fell prey to this scam almost all called the phone numbers on the job ad. Victims described their conversations with the con artists as "extremely convincing."
* Banks have a role in preventing this sort of scam, or at least they have a potential role. Multiple victims who fell prey to this scam

say they asked bank tellers for help and information before they signed an employment contract. The victims who went to their banks have told the World Privacy Forum that bank personnel told them that nothing was wrong. Preliminary findings indicate that if true this appears to be an emerging pattern among the victims. One victim worked at a bank, and even this individual did not understand how the scam worked in enough time to stop his own victimization.

B. How a Criminal Indictment Occurred

The victim who was indicted on theft charges follows along the same patterns as other victims of payment forwarding scams. The victim says she went online, found a selection of job ads in her profession, and applied for the jobs. She heard back from one of the employers and went through an email interview process in which, she, like the other victims, was asked to give up her bank account information.

The con artists told her that her job as a finance manager required that she transfer money deposits made to her personal bank account to a new account, therefore, she had to give up her bank account numbers. The victim says she called her bank and asked if this was ok. The victim signed the contract and sent it off via email. She received her first assignment from her employer, which was to transfer money overseas. She went to her bank to make the transfer, and was arrested on the spot.

She was charged with grand felony theft because the money she was about to forward was stolen. The stolen money actually belonged to an individual living in another state who had never had any contact with the job fraud victim. The victim was then indicted by a grand jury for the theft. She awaits trial and faces the real potential of prison time if convicted. This jobseeker is the first known victim of a job scam to be indicted and face actual criminal charges.

The challenge that job seekers will face in the future is to prove that they didn't "know better." Given that a bank employee has been fooled by this scam, it is not unreasonable to expect that this scam will continue to pull in victims that juries could say should have "known better." But job seekers who are not always computer crime experts, and online scams can fool very reasonable people.

IV. Timeline: The Evolution of a Job Scam

This timeline tracks one job scam as it systematically wove its way through dozens of job sites over the course of a year and left multiple victims in its wake. Like a computer virus, the scam has evolved over time. It is an ugly evolution that has substantially harmed job seekers who have fallen victim to it.

The scam began sometime in August of 2003, and as of July 7 2004, is still active. Known names this scam goes under are Unk Electronics, Macrocommerce Intersales, Nanjing Panada*, Antares Electronics, Inc.*, BestElectrics, and Omega Inc. Although the names are different, the likelihood is a very strong that it is all the same job scam.

It is likely that there are many more postings of these jobs than are listed below, but these are the instances the WPF is able to document conclusively.

(Note for text version of report: "PDF" is noted in this text version of the report to denote where documentation of the job listing is available in PDF form. To view the timeline with PDF documentation of the postings, visit the HTML version of the report:
The Evolution of a Job Scam.
http://www.worldprivacyforum.org/jobscamtimeline.html).

A. Timeline

2003

July 16

UNK Electronics job scam makes first known appearance at PickaJob - job listing PDF

September 17

UNK Electronics, Inc. job scam posted at JobSpider- New York.

job listing PDF

October 9

MACROCOMMERCE Intersales job posted at Careerspan.com — Dallas, New York, Sacramento

Full job ad PDF, Los Angeles; PDF.

Victim of UNK scam

Victim arrested, indicted for felony theft

November 11

MACROCOMMERCE posted at Preferredjobs.com - Atlanta; PDF.

November 18

UNK CareerBuilder - Dallas, Oregon; PDF

November 18

UNK posted at Chicago Tribune (via CareerBuilder) ; Unk Chicago Trib listing PDF.

November 18 (approx.)

MACROCOMMERCE posted at PickaJob.com - Phoenix, AZ; Phoenix PDF.

November 19

MACROCOMMERCE posted at CareerBuilder- San Francisco; PDF; New York, NY; PDF.

Victim of Nanjing Panada Electronics

Limited harm.

Victim of Nanjing Panada Electronics

Personal information stolen. Unknown consequences.

November 24

UNK posted at JobSpider - New York PDF. Jacksonville FL; PDF actual FL job ad ; PDF 2 of list; Houston Houston Job Ad PDF ; Nov. 24 JobSpider PDF ; Houston PDF 3.

MACROCOMMERCE posted at Jobspider - Cincinnati; PDF

Victim of UNK

Victim of Nanjing Panada Electronics

November 25

MACROCOMMERCE posted at CareerBuilder - Los Angeles; PDF.

November 30

MACROCOMMERCE posted at CareerBuilder - Cincinnati.Full job ad PDF; Miami PDF.

Victim of MACROCOMMERCE

December 1

MACROCOMMERCE posted at Preferred Jobs - Cleveland; PDF.

December 5

MACROCOMMERCE posted at CareerBuilder - Seattle PDF

December 10

WPF first learns of scam when it is contacted by Nick Corcodilos of Asktheheadhunter.com about the scam via a jobseeker tip-off.

December 11

WPF begins research on the scam. Finds MACROCOMMERCE job active at Jobvertise - Miami; PDF. PickaJob.com - Wash. D.C., Denver, San Francisco, Phoenix; PDF. The WPF found active postings (already detailed in the timeline) at CareerBuilder, Job Spider, Jobvertise, and PreferredJobs.

WPF Notified CareerBuilder, Pickajob, JobSpider, Jobvertise, Preferred Jobs of job scam and requested it be taken down.

December 12

Publication of WPF Consumer Alert (Jobseekers warned of jobs from Macrocommerce Intersales, Unk Electronics.) Alert was posted to site, sent to media. Consumer alert: http://www.worldprivacyforum.org/consfraudalert1.html. At the time the alert was published, the WPF only knew of job postings between November 20 and December 11, 2003.

Mid- December

NANJING posted at Monster.com, Unk ad tried as Nanjing Panada Electronics (email, Monster job #19846633)

WPF notified by jobseeker of new scam name, Nanjing Panada Electronics. WPF Alert updated to include Nanjing Panada Electronics.

2004

January 4; job reposting of Macrocommerce

MACROCOMMERCE reposted at CareerBuilder - Portland Maine Maine Job ad PDF; PDF listing; Atlanta, Philadelphia, Minneapolis; PDF job reposting ; Job repostings on same page as news reports of fraud PDF.

Victim, Jan. 6 from Maine, MACROCOMMERCE Ad via CareerBuilder.

Bank account numbers stolen, SSN. CareerBuilder notified by jobseeker of job scam.

Victim, ID Theft, fired from job due to victimization by the job fraud MACROCOMMERCE via CareerBuilder.

CareerBuilder notified by jobseeker of job scam.

January 8; job reposting of Macrocommerce

MACROCOMMERCE reposted at CareerBuilder -Minneapolis, Boca Raton, Kissimmee, Pompano Beach, Coral Springs, Miami Beach, Ft. Lauderdale, Lawrence, Massachusetts, Andover Massachusetts; PDF.

January 25; job reposting of Unk

UNK reposted at CareerBuilder - Kansas City; PDF.

January 26

Jobseeker email notifying World Privacy Forum of UNK ads exactly like MACROCOMMERCE showing up in Phoenix, AZ. (email)

February 1

ANTARES Antares Electronics, Inc. job ad makes first known appearance at CareerBuilder - Florida, Miami, Hollywood FL PDF

February 6

ANTARES posted at JobSpider - Salt Lake City PDF Miami, Cincinnati, Great Falls, Seattle PDF

February 12; job reposting of Unk

UNK reposted again at CareerBuilder - Baltimore; PDF; Atlanta, Maryland; PDF.

February 19; job reposting of Unk

UNK reposted again at Jobvertise - Huntington West VA; PDF; New Orleans; PDF.

March 10

ANTARES posted at MSN Careers- Ft. Lauderdale, Washington State; ANTARES posted at AOL Careerbuilder - Ft. Lauderdale, Philadelphia, Coral Springs PDF

ANTARES posted at CareerBuilder - Miami, Hollywood FL, Brementon, Yolo PDF

May 19

ANTARES posted at CareerBuilder - Seattle, Sacramento, Chicago, Detroit, Dallas, Orlando, Hollywood FL, Miami, Merrillville IN PDF

May 20

ANTARES posted at CareerBuilder - Philadelphia PDF

May 21

ANTARES posted at Jobvertise -- Detroit, Philadelphia, Chicago, Dallas, Sacramento, Seattle PDF

May 23

OMEGA Inc. posted at CareerBuilder -- Salem, OR PDF (also email) PDF Job listed as "Beta," contract comes back as "Omega Inc."

May 24

ANTARES posted at CareerBuilder - Sacramento, Philadelphia PDF, Seattle, Chicago, Dallas, Elgin, Newark PDF | PDF

May 30

ANTARES posted at Jobvertise - Philadelphia PDF

June 2

WPF Notified of UNK victim awaiting trial.

June 10

ANTARES Jobvertise - Detroit PDF

June 14

ANTARES CollegeRecruiter.net - Dallas PDF

BESTELECTRICS posted at CareerBuilder - Miami, San Francisco, Atlanta PDF

June 15

ANTARES posted at Withinmiles.com - Texas PDF

ANTARES posted at Lookingforwork.com - Texas PDF listing only

June 16

ANTARES posted at CareerMag.com - Texas PDF

June 16

BESTELECTRICS posted at Jobvertise -- New York City, San Francisco, Miami PDF

July 1

ANTARES posted at Lookingforwork.com - Texas PDF

ANTARES posted at CollegeRecuiter.com - Dallas PDF

July 3; job reposting of Macrocommerce

ANTARES found actively posted at Jobvertise PDF - Detroit, Philadelphia, Seattle, Sacramento PDF

BEST ELECTRONICS actively posted at Jobvertise PDF

MACROCOMMERCE actively posted at Jobvertise-powered site 206.221.233.36 - San Francisco, Indianapolis, Orlando, Dallas, Atlanta PDF

As of July 3 this scam was still operational. ANTARES Jobs were posted on Preferredjobs.com in Washington DC, Los Angeles, San Francisco, San Diego, Chicago, and Dallas. Other known job sites posting the ANTARES job ad include: AOL.com ,aftercollege.com , australiajobsite.com ,canadajobsite.com , careerspan.com, collegegrad.com (College Grad Job Hunter, Preferredjobs.com, Retiredbrains.com. Other known sites that posted Unk Electronics jobs during this time frame: dallasjobsite.com, jobs.pearlhaven.com, baltimore.4jobs.com, tutorgig.com.

B. Known Contact Names used in Scam

Known contact names used in this scam include:

Chan Hoi Wo: chan.hoi.wo@npehk.com (NANJING)

Wong Po Hang: Wong.Po.Hang@npehk.com (NANJING)

James Brownn (MACROCOMMERCE)

Thomas Becker: managerineurope@yahoo.com (MACROCOMMERCE)

Thomas Becker europeanmanagereu@yahoo.com MACROCOMMERCE

europeanagentseu@yahoo.com (MACROCOMMERCE)

europetraders2003@juno.com (MACROCOMMERCE)

futurebusiness200@yahoo.com (MACROCOMMERCE)

Ral Fernando (UNK)

Andrew Stevenson partner@antaresinc.org (ANTARES)

Business_italyeu@yahoo.com (ANTARES)

Italyagenteu@yahoo.com (ANTARES)

Helmud Luigi omegaincitaly@yahoo.com (OMEGA Inc.)

C. Note on Corporate Name-jacking

Antares Electronics Ltd. is the name of a legitimate company, as is Antares Technology Solutions. There may be other legitimate companies using the name "Antares." It is an unfortunate fact of scams that the scammers steal company names or names very close to legitimate companies in order to appear "safe." Additionally, Nanjing Panda is a legitimate company. Note that the scam company name was spelled very similarly to the real company name: Nanjing Panada is the scam spelling— there is an "a" added into the name to confuse job seekers.

At the time this report was published, Monster.com listed jobs from the real Antares employers. As of the last date checked, July 7, 2004, these jobs are not from fraudulent companies.

V. Job Site Responses

The World Privacy Forum contacted CareerBuilder.com, Monster.com and Hotjobs.com to invite them as industry leaders to provide information about how they protect jobseekers from fraud. These sites and others were also invited to participate in a joint teleconference to discuss possible solutions to job fraud, given the changed environment the industry now faces.

Monster.com, CareerBuilder.com, and HotJobs.com all responded with their job fraud plans. Monster.com and CareerBuilder.com said yes to the teleconference. At the time this report was published, researchers were waiting for an imminent response from HotJobs.com, which was in the midst of an earnings report and awaiting a final answer from parent company Yahoo!. Researchers expect to hear an answer from the company soon, and will update this section when an answer is received.

Some of the other sites contacted for the teleconference included Craigslist.org, which has agreed to participate in the teleconference, as has NACELInk, DirectEmployers, and PreferredJobs.

DICE was contacted to participate in the teleconference but declined participation.

Additionally, all of the sites posting the fraudulent jobs were contacted prior to publication of the report to notify them of the publication. A copy of the report and the timeline will be sent to all of the sites to assist them in removing the fraudulent jobs and hopefully removing this persistent scam.

Job site responses (listed alphabetically)

A. CareerBuilder Response

The vast majority of jobs posted on CareerBuilder.com are the result of the ongoing relationships our direct sales force has with customers. While job fraud is not a common occurrence at CareerBuilder.com, we take the issue very seriously and have implemented measures to help protect our job seekers:

[-] On every job posting, we include an alert for job seekers that provides tips to keep in mind when dealing with prospective employers.

The alert reads as follows:

[-] FOR YOUR PRIVACY AND PROTECTION, when applying to a job online:

1. Never give your social security number to a prospective employer.

2. Never provide credit card or bank account information, or perform any sort of monetary transaction.

Learn more >>
<http://www.careerbuilder.com/JobSeeker/Info/Privacy.htm>

[-] The alert links back to a special section on CareerBuilder.com that is devoted to Job Seeker Privacy and discusses what CareerBuilder.com does to protect job seeker information and what job seekers can do to protect themselves.
<http://www.careerbuilder.com/JobSeeker/Info/Privacy.htm>

[-] CareerBuilder.com includes this alert in our outbound emails to job seekers, which are distributed to millions on a daily basis.

[-] CareerBuilder.com has a dedicated team of Quality Control specialists who monitor job postings on our site on a daily basis. The team uses various search methodologies to identify any jobs that are in violation of our posting standards. If the team comes across a violation, the job posting will be promptly removed and the source will be "red flagged" to prevent the organization from submitting another posting in the future.

PDF of alert as seen on CareerBuilder job ad.

B. Hotjobs.com Response

(Note: Researchers did not find any iterations of the scam outlined in this report on Hotjobs.com.)

Yahoo! HotJobs put a strong process in place over a year ago to protect our job seekers from fraudulent job postings. I believe we are the only job board to proactively do this. We are constantly evaluating how we can protect job seekers and our customers. I listed some key points below.

[-] Fraudulent job postings violate HotJobs' terms of service

[-] As you can read in the Yahoo! HotJobs policy "Posting any franchise, pyramid scheme, "club membership", distributorship or sales representative agency arrangement or other business opportunity which requires an up front or periodic payment, pays commissions only (no significant salary) or requires recruitment of others including, but not limited to, members, sub-distributors or sub-agents is prohibited."

[-] We pride ourselves on protecting our job seekers from jobs that require the job seeker to make any type of investment or outlay of money.

[-] Any contract goes through a process where the company posting jobs is scrutinized for legitimacy (both internally and externally with parties who are also looking out for the best interest of the job seeker).

[-] We can't share the details in terms of how we screen for these types of jobs because we don't want our process to be manipulated.

[-] If fraudulent activity is brought to HotJobs' attention, we will take action to protect our job seekers including deleting any suspect job postings and blocking the access of the questionable job posters to HotJobs' site.

[-] While HotJobs is not aware of any incidents involving theft of personal information resulting from a job listing on the site, we still post information on HotJobs.com to protect our job seekers. We also send job tips to job seekers who receive the myHotJobs newsletter.

Here is a link http://help.yahoo.com/help/us/hotjobs/hotjobs-01.html to some of the content we post on the site to protect job seekers.

Essentially, we encourage job seekers to:

[-] Make informed decisions before sharing your Social Security number with a potential employer. Most employers will not ask for personal information until you arrive at their offices for an in-person interview and are given a formal job application, so be wary if you are asked to give your Social Security number by phone, e-mail or online.

[-] If you have doubts about a company's legitimacy, research the company using Web sites operated by the Better Business Bureau (www.bbb.org) and the United States Federal Trade Commission (www.ftc.org).

[-] Refrain from providing credit card or bank account numbers, or engaging in any financial transactions over the phone or online with a potential employer/recruiter.

[-] Withhold offering personal information (such as marital status, age, height, weight). Such questions violate federal hiring standards and job seekers are not obligated to answer them.

[-] Exercise caution when dealing with prospective job contacts outside of the United States.

C. Monster.com Response

Monster is aware of the rare occasions when fraudulent job postings have appeared on the site. We are proactively taking the steps necessary to protect our job seekers and provide a safe environment for them to manage their careers. In fact, Monster has a Fraud Task Force, overseen by senior management, that monitors the site for any suspicious activity. We implemented this safeguard not only to protect users, but also the integrity of the Monster brand and our website.

All job postings are screened and monitored to ensure their legitimacy. To assist job seekers, below are a few "red flags" that they should be careful of when viewing a job online:

[-] Email addresses from a non-corporate domain;

[-] Jobs involving Eastern European Countries; and

[-] Descriptive words in the postings including:package-forwarding, money transfers, wiring funds, eBay, and PayPal.

Monster will continue to work hard to protect visitors to our website. Last year, we sent an email to our entire user base, notifying them of the potential for fraudulent job postings and tips on how to protect themselves from falling victim to this rare occurrence. (The tips we have posted on our homepage are available via this URL: http://help.monster.com/besafe/). Most recently, we were made aware of a fraudulent email, posing as Monster, that was being distributed. The same day we were notified of this communication (from two of our job seekers), we alerted our entire active user base via the e-mail below.

PDF of Monster.com email alert to user base. (Note: this Monster email is not related to the scam discussed in this interim report.)

VI. Critical Tips For Job Seekers to Help Avoid Job Scams

The following four tips can help jobseekers protect themselves from falling prey to payment forwarding scams.

1. Never give personal bank account, PayPal, or credit card numbers to an employer.

2. Never agree to have funds or paychecks direct deposited to any of your accounts by a new employer.

3. Never forward, transfer, or "wire" money to an employer.

4. Do not transfer money and retain a portion for payment.

Legitimate employers do not need jobseekers' bank account numbers. While direct deposit of a paycheck is a convenience, if that is the only

option an employer offers, then jobseekers should not accept the job. A legitimate employer will give jobseekers the option of direct deposit, but not demand that it is used. Jobseekers should wait until they have met the employer in person before agreeing to a direct deposit option.

While some jobs may require an employee to make transfers for employers, legitimate employers making this request will go to extraordinary efforts to check the job seeker prior to making the hire. This would involve meeting the jobseeker in person and conducting rigorous interviews. This kind of job hire would not be made via email or even the telephone or a single meeting. Job seekers need to draw a line and understand that transferring money for employers is off-limits, period.

A. Known Red Flags

The UMAB payment forwarding scam contained what are now becoming known as "red flags" for job scams.

Red flags that should alert jobseekers to the presence of a job scam include:

1. Request for bank account numbers.

2. Request for SSN.

3. Request to "scan the ID" of a jobseeker, for example, a drivers' license. Scam artists will say they need to scan jobseekers' IDs to "verify identity." This is not a legitimate request.

4. A contact email address that is not a primary domain. For example, an employer calling itself "Omega Inc." will have a Yahoo! email address.

5. Misspellings and grammatical mistakes in the job ad.

6. Monster.com lists descriptive words in job postings that are tip-offs to fraud. Their list includes "package-forwarding," "money transfers," "wiring funds," "eBay," and "PayPal." WPF researchers also found that the term"Foreign Agent Agreement" often appears in contracts and emails sent to jobseekers.

Please see Appendix A for examples of what the emails and contracts for this kind of money transfer scam look like. The Timeline in Section IV has multiple examples of what the fraudulent job ads look like.

B. Most Effective Steps for Victims of Job Scams

Unfortunately, not everyone will escape job fraud in time. Jobseekers who are victimized by the UMAB scam and other payment forwarding scams are advised to take the following steps.

1. Close all bank accounts at the bank where the scam took place. It is a good idea to change banks to avoid "social engineering" attempts by the con artists to fool bank workers into giving out new account information.

2. Order a credit report from all three credit bureaus every 2 to 3 months. Watch the reports for unusual activity.

3. Victims of payment forwarding scams should contact their local Secret Service field agent. UMAB victims and other victims of payment forwarding scams should file a police report with local law enforcement officials as well.

4. Victims should report the company name, the job posting, and all contact names to the job sites where the scam was posted.

5. Victims should permanently close all email addresses that were associated with the job fraud.

VII. RSS Job Feeds and Job Fraud

RSS, a technology that collects information from Web sites, bundles it together and then sends it to individuals to read offline is gaining popularity. RSS stands for *Really Simple Syndication*or *rich site summary*. Right now, it looks like RSS may become an important part of how people use the Internet. For collecting and aggregating news headlines and tidbits from newspapers and blogs, RSS is convenient

and helpful. RSS does have the potential for some real drawbacks for job seekers unless it is thoughtfully deployed by job search sites. However, the drawbacks are a fairly simple matter to correct.

For example, the World Privacy Forum noticed that the site RSS-Job-Feeds.org collected and republished all of the fraudulent ads that appeared on CareerBuilder.com. RSS-Job-Feeds sent the ads straight to jobseekers without benefit of a privacy policy, contact information, or warnings about job fraud. It fed undiluted scams to jobseekers.

Another site, RSSjobs.com, pulls jobs from Monster.com, CareerBuilder.com, Hotjobs.com, DICE.com, Careerspan, the San Diego Union Tribune, the Boston Globe, and other sites. Researchers signed up to this site and tested it. The way it works is that the RSS feeds give users the headline of the job and some basic information about it. Then users click through the headline to see the actual ad. Some sites, such as CareerBuilder, post warnings on the actual job ads about job fraud. When users click on the job ad, they see the warning and tips. But not all sites do this. In the RSS environment, depending on how the site set up the RSS feed, a job seeker could potentially click on an ad and apply for the job without ever seeing a warning from the site.

RSS need not be a problem for job sites. It just needs to be considered very carefully and the feed should be configured to take job seekers back to the main site to view job ads. Job seekers need to be protected in the RSS environment. Sites can do this easily by making stand-alone information about job fraud available on every page containing a job ad.

VIII. Resources

* The December 12 consumer report relating to what became the UMAB scam may be found at <http://www.worldprivacyforum.org> and <http://www.privacyrights.org>
* FTC Help Line: Call this number to file a complaint about fraudulent jobs. (877) 382-4357.
* World Privacy Forum http://www.worldprivacyforum.org
* Privacy Rights Clearinghouse:http://www.privacyrights.org
* NACAA (National Association of Consumer Affairs Administrators) can help job seekers find consumer help in their region: http://www.nacaanet.org/

* United States Amended Law enacted by Congress showing ID Theft Prevention Law and Credit Restoration Law for Victims--This can be located on the Better Business Bureau Website along with several other Scam, ID Theft, & Fraud references. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:h2622enr.txt.pdf
* BBB Explanation of new laws that protect identity theft victims: http://www.bbb.org/alerts/article.asp?ID=483
* Credit Bureaus: Equifax: (800)-685-1111 Experian (888) 397-3742 TransUnion (800) 888-4213

IX. Credits

Thank you to all of the job seekers who have contacted the WPF and shared their experiences with us. Without the UMAB victims' information, researchers would have had much greater difficulty piecing together the puzzle this scam presented.

Thank you to Beth Givens and Jordana Beebe of the Privacy Rights Clearinghouse.

Thank you to Michael Shamus of Utility Consumers Action Network.

Nick Corcodilos of AsktheHeadhunter.com alerted the WPF to the original iteration of the scam which was the scam researchers eventually selected for the longitudinal study. Without Nick Corcodilos, there would have been no substantial documentation of the UNK iteration of the UMAB scam, and maybe not even the Macrocommerce iteration.

DDT of Cryptorights.org provided researchers with technical and informational support.

DSP of Privacy Activism provided key insight and information.

Thanks to NACAA for generously allowing Pam Dixon the opportunity to discuss the UMAB scam at their national conference. The conversations at NACAA were helpful in gaining an understanding of the broad national impact of job fraud.

John Boak designed the timeline and was critical to the design of the visual presentation of the research information.

X. Methodology

The World Privacy Forum began study of online job scams in February 2003.

1. Researchers did a background material search for information and collected and read background material on how job scams operated from sources such as newspapers, online news sites, law reviews, consumer protection agencies, the BBB, the FTC, and the U.S. Postal Inspector General.

2. A search for open fraud cases was conducted nationwide.

3. Twenty job sites that varied in size and focus were selected as a first study group.

4. A preliminary study was conducted.

    a. Suspicious ads were collected and studied.

    b. After suspicious ads were seen on multiple sites, researchers applied to the job ad to confirm whether or not it was a scam.

c. If the job came back with a request for funds, the job was concluded to be a scam.

5. Researchers chose a two-phase study model. Phase one was to study a single scam longitudinally. Phase two was to study the overall incidence of fraud across multiple sites in terms of percentages and type.

6. Phase one began in November 2003. A group of known scams were considered.

7. Researchers selected a particularly widespread scam to track.

a. Fifteen search engines were used methodically to search for multiple linguistic patterns found in the target ad/scam.

b. Researchers used company names, email addresses, contact names, and phone numbers found in the ads to search for the ad via search engines.

c. A group of control job sites were also checked regularly for incidences of the ad being posted.

i. If the ad was found "live" researchers applied to the ad under multiple names.

ii. If the ad was found after the fact, researchers documented the ad via cache and screen captures for documentation that it was posted.

iii. Contracts and emails resulting from job applications were documented and compared.

d. When researchers found incidents of the job ad being reposted "live," those incidents were documented then reported to the job site.

8. Victims of the tracked scam were interviewed and asked to send documentation of applying to the job and so forth.

9. Company names were checked against legitimate company names.

10. Ads were compared for similarities in language, email exchanges, employment contract details, and other details.

11. A timeline was constructed of all documented ads that were strongly linked by enough factors to create reasonable certitude of it being part of the same scam "string."

Appendix A: From the Victims' Perspective: Sample UMAB contracts and email exchanges.

The timeline has many examples of what the job ad looked like. Below are step by step examples from UMAB scam victims of how they were led through the process of this scam after responding to one of the fake ads.

I. Email Exchanges from two victims of the Macrocommerce Intersales version of the scam

A. Step One:

After replying to the job ad, an email similar to the one below was sent to victims. The following email is from the Macrocommerce Intersales version of the UMAB scam. The victim this was sent to lived in Maine at the time.

(Misspellings were not changed)

Dear sir,

Please let me to introduce myself, I am James Brown, sales representative of the Macrocommerce Intersales Company based in Berlin, Germany. Our company is looking to sign a Company / Foreign Agent Agreement in order to deposit their U.S sales founds into a company / individual US bank account. Our company agrees to deposit founds into a company / individual US bank account if the company

/individual agrees to accept, 5 % of these founds as payment for services. The company /individual is then responsible for wiring the remaining 95% of the founds to one or more of the three designated local distributors. The service fees associated with wiring these founds will be deducted from the 95 % sent back to the company or the company's designated local distributor.

In order for us as a company to deposit these funds into the U.S bank account we will be needing full info of the U.S bank account as:

1-ACCOUNT HOLDER'S NAME AND ADRESS

2-ACCOUNT HOLDER'S TELEPHONE NUMBER

3-BANK ACCOUNT NUMBER

4-ROUTING NUMBER

5-THE BANK ACCOUNT ISSUER(BANK WHERE THE U.S ACCOUNT IS OPENED)

6-BANK ADRESS

7-BANK TELEPHONE NUMBER

If you as a manager of a company or as an individual wish to sign a Company / Foreign Agent Agreement in the condition above mentioned please contactour department in order to send more information about the Foreign Agent Agreement papers work. We look forward to you partnership. Thank you for your time and understanding.

James Brown Sales Representative

Macrocommerce Intersales Company

Oranienburger Strasse 114

10 999 Berlin

Germany

0049/16092469119

B. Step Two: Request from Con Artists for Making Transfer of Funds

The following email was sent to a Texas-based victim of the Macrocommerce Intersales version of the UMAB scam. The email tells the victim how and where to transfer the money. This email is a good example of the kinds of things a con artist will request of a victim caught in a payment forwarding type of scam.

(Misspellings were not changed).

From: Foreign Agent

<foreignagent@macrocommerce.org>

To: xxx

Subject: Re: Incoming wire

Date: Mon, 5 Jan 2004 17:02:36 -0800 (PST)

Dear sir,

As soon as the money clears cash out the money that you have recived ($9600) and go to a Western Union Office and send the money to our company distributors as follows:

Here are the names of our Company Distributors where you will wire the money to via Western Union Money Transfer.

PETER ANDERSON

Street: Lijnbaansgracht 163

Zip code: 1016 VX

City: Amsterdam

Country: Netherlands

RENY STEVENSON

Street:Oudezijds Armsteeg 12

Zip code:1012 GP

City: Amsterdam

Country: Netherlands

ERNANDO BECKER

Street:De Wittenkade 120

Zip code :1012 DW

City: Amsterdam

Country:Netherlands

From the $9600 you keep please $480 for you. The other $9120 please split them to the three Company Distributors, the fees for the western union are include to the $9120 ! After that please let us as soon as posible know the MTCN # of each transfer from each name of our Company Distributors !! I want you to send the money to Netherlands because we need to pay for a new headquarter space in Amsterdam.

Notice: Doesn't matter what the western union says about not transfering a amount like more that 2000 us $, cause in the past some nigerian mafiosis ripp a lot of money. but we do all our busines through western union int about 150 000 US $ each week.

Hope to hear from you as soon as posible.

Thank you for your time and understanding.

II. Example of how the same job scam operates under different names

The following email came from a potential victim who replied to a job ad from Omega Inc. The contract that Omega Inc. used is exactly the same contract that Macrocommerce Intersales used, complete with misspellings and unique grammatical errors. The job ad itself was slightly different, but it had certain key similarities and the posting pattern was the same as the UMAB scam. The contract below is confirmation that the company name of Omega is related to the UMAB scam.

(Misspellings were not changed).

Dear sir,

Please let me to introduce myself, I am Helmud Luigi , sales representative of the OMEGA INC based in ROMA , ITALY. Our company is looking to sign a Company / Foreign Agent Agreement in order to deposit their U.S sales founds into a company / individual US bank account. Our company agrees to deposit founds into a company / individual US bank account if the company /individual agrees to accept, 5 % of these founds as payment for services. The company /individual is then responsible for wiring the remaining 95 % of the founds to one or more of the three designated local distributors. The service fees associated with wiring these founds will be deducted from the 95 % sent back to the company or the company's designated local distributor.

In order for us as a company to deposit these funds into the U.S bank account we will be needing full info of the U.S bank account as:

1-ACCOUNT HOLDER'S NAME AND ADRESS

2-ACCOUNT HOLDER'S TELEPHONE NUMBER

3-BANK ACCOUNT NUMBER

4-ROUTING NUMBER

5-THE BANK ACCOUNT ISSUER(BANK WHERE THE U.S ACCOUNT IS OPENED)

6-BANK ADRESS

7-BANK TELEPHONE NUMBER

If you as a manager of a company or as an individual wish to sign a Company / Foreign Agent Agreement in the condition above mentioned please contactour department in order to send more information about the Foreign Agent Agreement papers work.

We look forward to you partnership.

Thank you for your time and understanding.Helmud Luigi

Sales Representative

OMEGA INC

STAZIONE TERMINI GALLERIA CENTRALE BIN,

13/14 LATO VIA GIOLITTI

ROME

00185

ITALY

Tel: (39) 80060143

omega incitaly [omegaincitaly@yahoo.com]

EndNotes

1. EQuest Press Release "eQuest Surpasses 24 Million Job Posting Transactions in 2002." <http://www.equest.com/membership/merger_news_milestone.asp?>. July 7, 2004.

2. For example, in February-March 2003, Monster.com sent out emails to its user base warning of fraudulent job postings. It and other sites added new or strengthened job fraud warnings to their sites at that time. See Associated Press "Monster.com warns jobseekers of ID Theft," Adam Geller, February 27, 2003 documenting these events.

3. See for example a student described in a New York Times article on job fraud victims. New York Times, "Fraud in Online Job Listings" Bob Tedeschi, May 17, 2004. The student did forward stolen money unwittingly.