MEDIA ADVISORY
CONSUMER FRAUD ALERT

For Immediate Release
December 11, 2003

Bogus Job Ads Attempt to Obtain Consumer Bank Account Data

World Privacy Forum
2033 #402 San Elijo Avenue
Cardiff by the Sea, CA 92007
Pam Dixon
(760) 436-2489
info2004@worldprivacyforum.org
www.worldprivacyforum.org

Privacy Rights Clearinghouse
3100 Fifth Ave., Ste. B
San Diego, CA 92103
Beth Givens
(619) 298-3396
bgivens@privacyrights.org
www.privacyrights.org

The World Privacy Forum and the Privacy Rights Clearinghouse have become aware of a nationwide job scam currently in action. We are advising job seekers to avoid any response to job ads coming from **Macrocommerce Intersales** and to be aware of the high potential for financial fraud and /or identity theft if they have already responded to job ads from this company.

Background

Macrocommerce Intersales has posted a variety of jobs nationwide on CareerBuilder.com, Pickajob.com, TheJobSpider.com, Jobvertise.com, and on job banks specific to the cities of Seattle, Boston, New York, Cleveland, Detroit, San Francisco, Denver, Atlanta, Miami, Chicago, Cincinnati, Sacramento, San Diego, Los Angeles, Atlanta, Jacksonville, Orlando, and for all of Florida. (For example, losangelesjobbank.com, atlantajob.com, atlantapreferredjobs, etc.) Most of the job sites have posted from one to four jobs from the company.

The fraudulent jobs were posted as early as November 20, 2003, and as recently as December 11, 2003. Typical wording for the job is “Electronics Company looking for a finance manager in USA” with a salary of $50,000- $70,010. Samples of how the jobs look as posted are available in PDF format at www.worldprivacyforum.org.

The job ads request applicants to send a resume and an email to managerineurope@yahoo.com or to foreignagents@macrocommerce.org. A “Thomas Becker” then sends out a request for more information. The email, below, reveals that Macrocommerce is engaging in an old-fashioned check fraud scam wrapped in new clothing. Unfortunately, the World Privacy Forum is aware of at least two people who have been caught in similar types of scams in the past year.

Following is the email researchers at the World Privacy Forum received after responding to the Macrocommerce job ad: (Spelling has not been corrected.)

> **From:** Foreign Agent <foreignagents@macrocommerce.org>
> **Date:** Thu Dec 11, 2003 1:10:58 AM US/Pacific

To: (removed)
Subject: Re: job opportunity

Dear sir,
Please let me introduce myself,
I am Thomas Becker, 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.
Your annual salary will be between $50.000 and $70.000.The only thing that you as our foreign agent will have to do is send the amounts that you recive from our sales ,to our designated local distributors.
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 ADDRESS
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 ADDRESS
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 contractor 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.

Thomas Becker
Sales Representative
Macrocommerce Intersales Company
Oranienburger Strasse 114
10 999 Berlin, Germany
0049/16092469119

Job Search Safety Tips

We know of four specific instances of fraudulent job ads being posted on online job search sites. This is one of them. Because fraudulent job ads appear to be "slipping through," it is important that whenever looking for a job online, job seekers remember to be extremely cautious about responding to job ads, especially for jobs overseas. Just because a job ad is on a well-known job site does not mean the job is not a scam.

Below are the key tips for identifying job scams before you get snared. Please see **Fact Sheet 25** at the Privacy Rights Clearinghouse for more detailed tips www.privacyrights.org/fs/fs25-JobSeekerPriv.htm.

The 2003 Job Search Privacy Study at the World Privacy Forum has additional information about job searching and privacy www.worldprivacyforum.org; also, www.jobsearchprivacy.org has information specifically about online job search privacy.

How to Detect Bogus Job Ads

According to Pam Dixon of the World Privacy Forum, key indicators of job scams are the following:

1. After responding to the job ad, the company wants job seekers to give up highly personal information via email. Unfortunately, many legitimate companies are beginning to ask for highly personal information from job applicants via email. This makes it more difficult to weed out the scams. In general, never give up bank account information, credit card information, or physical details about eye color, height, hair color, etc.

2. A company asks for SSN or bank account information via email.

3. The company is less than one year old.

4. The website for the company that is indicated by the sender's email address does not exist or is "under construction."

5. A check of the domain name of the company in www.domainwhitepages.com gives highly contradictory information. For example, Macrocommerce says it is a European company based in Berlin, Germany. But a check of www.macrocommerce.org on domainwhitepages shows that Macrocommerce is actually based in Maryland and is owned by someone other than Macrocommerce. You may be dealing with a subsidiary of a company, or you may have found a problem. **When you find contradictory ownership information combined with a request for bank account numbers, consider the job ad a fraud and don't respond to it.**

6. Although it is not always an indicator of fraud, notably poor spelling throughout a job ad can tip you off that there may be a problem, especially when found in conjunction with other factors such as no Web site, etc.

What to Do if You have Already Responded to the Macrocommerce Ad

If any job seekers have received and responded to this email or company, we recommend that you take proactive steps to protect yourself from harm.

Beth Givens of the Privacy Rights Clearinghouse recommends that affected job seekers take the following steps to combat this type of fraud:

1. Cancel the bank account in question.

2. Get a new account and put a password on your new account. Avoid using easily guessed or discovered passwords. Mother's maiden name, date of birth, SSN, and pets' names are examples of weak passwords. Instead, make up a phrase that is easy to remember. "A marathon run," "notebook paper," and other such simple phrases are much stronger passwords and provide more protection.

3. Watch all existing bank accounts very carefully in the coming months, and order a credit report. You may do this by calling the three credit reporting bureaus, Equifax at (800) 685-1111, Experian at (888) 397-3742, and TransUnion at (800) 888-4213.

4. If you believe your Social Security Number is compromised, you would typically place fraud alerts at the three credit bureaus. However, this scam does not appear to compromise the SSN. If you wish, just to be on the careful side, you may still want to put fraud alerts on as a pro-active measure. That way if somebody attempts to obtain credit in your name you will be contacted by the credit issuer. Equifax at (800) 525-6285, Experian at (888) 397-3742, and TransUnion at (800) 888-4213.

5. If you decide not to put a fraud alert on your credit report, be sure to order your credit report in the next three months just to make sure that your financial identity has not been compromised.

6. Notify the Web site hosting the job about the scam. This way, they can take appropriate action by either removing the offending ad and/or making sure the person who posted the ad is no longer able to do so on their site.

7. File a complaint with the Federal Trade Commission (FTC) by going to their website at www.ftc.gov and clicking the link in the upper navigation bar for File a Complaint or by calling the FTC at (877) 382-4357.

8. File a complaint with the FBI's Internet Fraud Complaint Center at www.ifccfbi.gov.

For more detailed information about how to handle identity theft, please see **Fact Sheet 17A** at www.privacyrights.org/fs/fs17a.htm. For general privacy information, please see www.privacyrights.org.

##30##