



Special Report Special Report Special Report Special Report

Recent Scams Prey Upon
Your Corporate Goodwill

MEMA Brand Protection Council

June 2008

Recent Scams Prey Upon Your Corporate Goodwill

Theft of your intellectual property may not be limited to counterfeit goods. A recent string of fraudulent e-mail and mail scams have revealed a new concern for business entities – corporate identity theft.

By incorporating a company's logos, trade names, and even employee information, thieves are trading on an organization's goodwill and reputation in order to gain access to consumer data. These scams potentially tarnish an organization's name and may lead consumers to call into question a company's business practices.

One such scam recently hit LG Electronics, the manufacturer of televisions and home electronics. The scam consisted of a "Job Offer" e-mail that was disseminated from several e-mail addresses that appeared legitimate because they incorporated the LG name.

For instance, one batch of the e-mails was sent by "info@lgelectronicstore.com." The text of the e-mail identified a legitimate Indian office of LG Electronics and described the dream job – flexible hours, the ability to work from home and a monthly salary of \$10,000. The e-mail also included LG Electronics' logos and provided employee information. It appeared to be an authentic job offer.

In another instance, Bendix Commercial Vehicle Systems LLC and Bendix Spicer Foundation Brake LLC, manufacturers of commercial vehicle safety technologies, were hit by a sweepstakes scam. In the scam, a third party sent – via U.S. mail – a false sweepstakes offer that included the Bendix name, logos and fake reward checks.

The letter explained that the recipient could contact Bendix for more information and provided a fake phone number. This scam hit Bendix twice in a two-month period and the second round of letters indicated that the recipient had "won" the sweepstakes and that they could cash the check.

These scams display a new level of sophistication and attention to detail that has many corporate executives scratching their heads. The fake "Job Offer" e-mail included legitimate employee contact information and pictures. The fraudulent sweepstakes offer included a fake check displaying the MELLON BANK name.

Typically, scammers are taking these steps to appear legitimate in an attempt to gain access to consumer personal data. When a consumer replies to the offer, "clicks here" or contacts the company by phone, he unknowingly gives the scammer access to certain personal data. By using a recognized corporate name as a guise, they have an easier time gaining that consumer's trust and feel protected from legal scrutiny, at least initially.

Executives can take steps to ensure their corporate identity is not tarnished by a scam. For starters, an organization can include a notice on its Web site that identifies an e-mail address or phone number that consumers can use to confirm the legitimacy of an advertisement or offer. This will allow you to quickly learn about any false offers that incorporate your organization's name.

What to Do if Your Company Is Hit by Corporate Identity Scammers

If and when you do learn about a scam, you must act immediately to notify consumers. The notice should be posted on your company's Web site and disseminated by e-mail or mail, depending on the method that the scam was sent. For instance, if the scam was sent by U.S. mail, the notice from your company should also be sent by U.S. mail.

The notice should provide as many details as possible – dates, content and a description of the offer. If the fake offer duplicates a legitimate offer disseminated by your organization, the notice should give information to assist the consumer in distinguishing the legitimate offer from the fake one. If it is too difficult to distinguish the two offers, an organization should consider retracting the original offer.

Simultaneous with the public notice, a company hit by such a scam should notify the authorities. Depending on the type of scam – whether e-mail or U.S. mail – different federal agencies may be involved.

In the case of online scams, for example, your company could file a complaint with the Internet Crime Complaint Center (IC3), at www.ic3.gov. The IC3 is a partnership between the FBI, the National White Collar Crime Center and the Bureau of Justice Assistance. It is essentially a forum that was developed by these organizations to receive, develop and refer complaints involving cyber crimes. An organization also can contact the host of the e-mail address that disseminated the scam – such as Yahoo, AOL or Google – to have the account disabled.

For scams sent via U.S. mail, a company can report the scam to the U.S. Postal Service. The contact details can be found on the U.S. Postal Service Web site at www.usps.com/postalinspectors/fraud/ContactUs.htm.

Finally, a company should also consider reporting the scams to the Federal Trade Commission (FTC), www.ftc.gov. The FTC may not be able to take action against the person sending the offer, since these scams are not typically within their legal jurisdiction. But by putting the FTC on notice, you are giving notification that your company did not disseminate the offer and that you are taking action in the event a consumer lodges a complaint.

Arent Fox is monitoring this issue. If you have any questions, please contact Marc Fleischaker or Sarah Bruno.

Marc Fleischaker
fleischaker.marc@arentfox.com
202-857-6053

Sarah L. Bruno
bruno.sarah@arentfox.com
202-775-5760

For information on the MEMA Brand Protection Council, call Jack Cameron at 919-406-8856 or e-mail jcameron@mema.org.