

**DON'T LET YOUR CUSTOMERS  
GET HOOKED BY "PHISHERS"**

**IN THIS ISSUE:**

- **Don't Let Your Customers Get Hooked by "Phishers" ....1**
- **When in Doubt, Don't Throw it Out—The Importance of Document Retention.....2**
- **Overtime Pay Tug-of-War Continues.....2**

Identity theft through "phishing" has raised so much concern that the federal banking regulators issued a brochure on September 8, 2004 to help consumers understand and avoid it (see www.frb.gov).

**"Phishing" Defined**

According to Webopedia, "phishing" is the act of sending an e-mail falsely claiming to be an established legitimate business (such as your company) in an attempt to trick the recipients into sending their private information to the con artist who sent the e-mail. The recipients are asked to send information, usually by clicking a link to a fraudulent, but authentic-looking, website.

**How it Works**

These fraudulent e-mails and websites appear almost identical to legitimate e-mails and sites and sometimes even include seals and logos taken from the legitimate sites. In fact, a recent study shows that 92% of phishing attacks utilize "spoofed" e-mail addresses and websites, making them appear as though they are from a legitimate address while hiding their actual addresses. In one case, e-mails claiming to be from eBay told recipients that their accounts would be suspended immediately unless they sent updated credit card information to a fraudulent website link provided in the e-mail.

**Phishing Costs**

Phishing has already become an expensive and extensive problem. According to recent reports:

- Phishing attacks cost U.S. banks and credit card issuers approximately \$1.2 billion last year.
- Costs of just one phishing incident can easily exceed \$1 million.
- Phishers are able to get responses from up to 5% of recipients.

A phishing attack can end up costing a company in customer reimbursements, IT Department time, and lost productivity to resolve the situation. Furthermore, these costs do not reflect the unquantifiable harm to a company's reputation as a trustworthy or secure place to conduct business.

**PHISHING ATTACKS COST U.S. BANKS AND CREDIT CARD ISSUERS APPROXIMATELY \$1.2 BILLION LAST YEAR**

Phishing attacks also seem to be on the rise, with a recent report noting that phishing attacks increased nearly 4,000% since November 2003.

**Phishing Grounds**

The financial services sector seems to be the industry most targeted for phishing, by number of companies targeted and total number of attacks, according to an anti-phishing group. Citibank was the most targeted organization as of June 2004, with Bank of America, US Bank, PayPal, Bank One, FleetBoston Financial and MasterCard also experiencing persistent attacks. As recently as last week, SouthTrust Bank warned customers about a phishing scam targeting them.

**What You Can Do**

To limit your company's vulnerability to phishing attacks, anti-phishing groups have suggested the following:

- Maintain ownership of your company's domain name and gain control over similar-sounding domain names.
- Monitor the internet for suspicious uses of your company's name and images on websites and in spam e-mails.
- Use and routinely update appropriate anti-virus software to detect viruses that could access your customer e-mail list.
- Warn your customers not to respond to unsolicited e-mail requests for personal financial information.
- Urge customers to ensure that they are using a secure website (one that begins with "https://" instead of just "http://") when submitting sensitive information. Criminals are now able to successfully copy the legitimate "secure site" logos (e.g., the "closed padlock" symbol) from trusted companies and paste them on their fraudulent sites.

These steps are, of course, in addition to the usual anti-fraud measures that companies employ.

**A company can take specific steps to reduce the possibility of successful "phishing" attacks that could harm its customers and tarnish its reputation as trustworthy and secure.■**



## WHEN IN DOUBT, DON'T THROW IT OUT—THE IMPORTANCE OF DOCUMENT RETENTION

As highlighted by two recent cases, companies need to consider whether and when to suspend their document retention policies when faced with even just the possibility of litigation.

In the first case, a Fortune 50 industrial company was ordered to pay \$2.75 million in sanctions for



destroying e-mails related to an ongoing lawsuit. While the company had in place a document retention policy that routinely permitted the deletion of e-mails over 60 days old, it failed to halt this practice for e-mails that might have been relevant to the lawsuit. Instead, the company continued the deletions for two months in violation of a court order and failed to notify the court for four months about the deleted e-mails. The Federal district court cited the company's "reckless disregard and gross indifference" as reasons for such a high monetary sanction.

In the second case, a different Federal district court sanctioned a New York-based financial services company for, among other things, allowing the loss or destruction of e-mails on its

system that were relevant to an ongoing lawsuit in which the financial services company was a defendant. While the company and its counsel suspended the company's document retention policy, the court found that counsel also should have taken affirmative steps to preserve the electronic communications.

As a result, the court (i) ordered the company to pay certain litigation costs of the plaintiff and (ii) instructed that the jury could infer that the missing e-mails would have been unfavorable to the defendant's case.

**The crucial issue that a company must address in each instance is when and how to suspend its document retention policy once the company "reasonably anticipates" becoming involved in litigation. ▣**

## OVERTIME PAY TUG-OF-WAR CONTINUES

*Alan Rupe of our Wichita office writes:*

On September 9, 2004, the U.S. House of Representatives passed an amendment to the \$470 billion Labor-HHS-Education appropriations bill to rescind the Bush Administration's new overtime policy, with one exception. A provision that guarantees overtime compensation to any worker earning a base salary of \$23,660 or less would be the only provision preserved.

Sponsored by Congressmen

**The Department of Labor stated that the regulations will "strengthen overtime rights for 6.7 million American workers, including 1.3 million low-wage workers who were denied overtime under the old rules," but critics claim that the new regulations could actually deny millions of workers any overtime pay**

George Miller (D-California) and David Obey (D-Wisconsin), the bill was approved by a vote of 223-193.

Even if the U.S. Senate approves the bill, the battle over overtime will continue, as the White House has vowed to veto any bill containing language that affects the overtime regulations that went into effect on August 23, 2004. For a summary of these new regulations and their implications, see our publication on our website at <http://www.kutakrock.com>, or e-mail us and we will send it to you.

The new regulations are complex and have already generated questions about their scope and application, especially as workers find out they are no longer eligible for overtime.

**The outcome of the repeal effort remains uncertain, so companies should continue to focus their efforts on implementing the new regulations. ▣**

Kutak Rock LLP is a national law firm with 16 offices located throughout the United States. Our practice areas include:

- Corporate Transactions
- Federal Bank Regulatory Matters
- SEC Reporting and Compliance
- Mergers and Acquisitions
- Bankruptcy / Creditor's Rights
- Employment Law
- Commercial and Securities Litigation

Please visit our website  
[www.kutakrock.com](http://www.kutakrock.com)  
to learn more, or contact:

**Paul Borja.....202-828-2310**  
[paul.borja@kutakrock.com](mailto:paul.borja@kutakrock.com)

**Jeremy Johnson....202-828-2463**  
[jeremy.johnson@kutakrock.com](mailto:jeremy.johnson@kutakrock.com)

Editor:

**Justa Schmidt.....202-828-2305**  
[justa.schmidt@kutakrock.com](mailto:justa.schmidt@kutakrock.com)