



Kevin M. Busch is the chair of our commercial department and a member of our board of directors. As part of his commercial practice, Kevin counsels banks and their customers regarding all aspects of banking law, including check fraud problems. He may be reached at BuschK@moss-barnett.com or 612.877.5292.



IN THIS ISSUE

Page 1:

Internet Fraud —
Don't be the Next Victim

Page 2:

Minnesota Law on WCCO Radio

Page 3:

Employment Law Alert
Increased Liability for ERISA-
Plan Administrators

Page 4:

Role Reversal: Caring for
Aging Parents

Page 6:

Energy Conservation at
Moss & Barnett

The internet has become an integral part of business and personal life for many of us. But the speed, low-cost, and anonymity that characterize the internet have attracted criminals worldwide, intent on separating you from your money and stealing your important personal information.

A bit of knowledge regarding the criminals' tricks and a strong dose of skepticism will help you protect yourself. Let's look at a few of the common tricks:

Phishing. Criminals *fish* for important personal information using *phony* addresses and web sites. You might receive an e-mail that appears to be from your bank, or the IRS, or a government regulator. The e-mail may have an exact replica of the logo of the bank, the IRS, or the regulator and will appear official and urgent. It may have some accurate details about you. It will ask you to reply to confirm various details about you, your account, and your social security number. **DO NOT RESPOND.** These e-mails are *NEVER* legitimate. No bank, governmental agency, or other entity that legitimately needs your personal information will ever ask you to disclose information through an e-mail.

The Hot Stock Tip. An unsolicited stock tip might be legitimate, but it almost certainly is not a good deal. Ask yourself why someone who does not know you would suddenly decide that you, out of hundreds of millions of internet users, should be given the chance to make a killing in the stock market.

The Lottery. Congratulations! You're a winner! Just fill out this form to collect your prize. And please include a minor \$25.00 fee to cover taxes and postage. **DO NOT SEND THE FEE.** There is no prize. Anyone who does respond will be asked to pay an endless series of fees and will never receive any real prize.

The Overpayment. This scam has a couple of variations. Perhaps you just sold something on one of the on-line auction services. Or, your business has been asked to help another business collect on some old debts. Or, you have been asked to let some foreign governmental official clear some money through your bank account because the money has been trapped in a foreign country due to an untimely death or a political coup. A large cashier's check will arrive and you will be instructed to deposit the check, take out your share, and wire transfer the balance to a bank account out of the country. **DO NOT GET CAUGHT IN THIS TRAP.** The cashier's check is phony, but you and your bank will not discover that it is phony for a week or two. The wire transfer cannot be recovered after it is sent. When the cashier's check bounces, *YOU* will have to reimburse your bank for the amount of the check.

The internet is a valuable tool, but it must be used wisely. If you receive an internet offer that seems too good to be true, or if you are being asked to act too quickly, stop immediately. Seek out advice from a trusted friend, banker, accountant, or lawyer. A bit of extra time to think about the request or offer will probably convince you not to participate.