THE CHRISTIAN SCIENCE MONITOR csmonitor.com

from the April 02, 2007 edition - http://www.csmonitor.com/2007/0402/p13s02-wmgn.html

Step cautiously into an online bank

Interest rates and convenience are high, but so are security concerns. And customers have to be especially vigilant.

By G. Jeffrey MacDonald | Correspondent

For savers looking to get the highest possible interest rates on their cash holdings, the call of the Internet keeps getting louder.

In March, ING Direct launched nationwide the first completely electronic checking account. Depositors receive 4 percent interest on balances up to $50,000 and have no minimum requirements. This month, HSBC plans to roll out its own high-yield electronic checking account with an interest rate that's soon to be announced.

High-yield checking accounts mark the latest enticing offer from a universe of about 60 domestically registered virtual banks, which conduct business online rather than in brick-and-mortar operations. Virtual savings accounts now routinely pay 5 percent or more. Deal hunters are also finding mortgages with reduced fees and higher than average rates on certificates of deposit.

Taking advantage of virtual bank products, however, involves more than just a few clicks of the mouse. Vigilant maintenance of computer security systems is a must for anyone with a virtual account, say bankers and security experts. And even then, experts differ about what's the best way to manage accounts in order to maximize returns while minimizing risks.

Some financial advisers urge clients to follow the money. A person who isn't carrying high-interest debt and wants to keep cash on hand for a rainy day should consider putting most of the cash in virtual accounts, according to Bill Driscoll, a financial planner in Plymouth, Mass. The reason: high returns and low risk.

"There's absolutely no commitment. Why wouldn't you take advantage of it?" Mr. Driscoll asks. On the matter of security, he says, "You have just as much risk in a regular bank as you do with an Internet bank [because] they're all using the Internet for electronic information and for transmitting data."

But others disagree. Security consultant Andrew Colarik, who has written three books on cyberterrorism, says anyone with a virtual account should use it solely to pay one month's bills and keep the rest in accounts that aren't accessible online. That way a depositor limits risk of loss, he says, since "we keep taking for granted that all of this technology has been perfected, and it hasn't been."

"A higher interest rate means a higher risk, and somehow we have disconnected this" from current thinking about virtual banks, Mr. Colarik says. "If there is a breach, if there is a violation, what is your recourse?" In most cases, he says, chances are "you lose your money."

To date, the largest Internet banks report solid safety records. HSBC and ING Direct, for instance, both say they've never had a customer lose any funds due to a security breach. And even when Emigrant Direct's website was down for days last summer, customers didn't lose their money, although some complained of difficulty accessing funds.

What's more, in an age of concerns about identity theft, some advisers believe clients are actually more secure using virtual banks. The absence of a paper trail, which follows traditional banking transactions, reduces the likelihood that a thief will find valuable account numbers or passcodes in garbage bins, according to Justin Pritchard, a financial planner in Denver. And even paper checks have their downsides.

"It's worse to hand someone your paper check than it is to hand someone your user name and password of your online account," says Jim Bruene, editor of Online Banking Report, an industry newsletter. "That paper check not only has all your [contact] information on it, it has your checking account number on it. Your bank account number is right there, printed on the check," which could enable a counterfeiter to manufacture checks and drain an account of funds.

Virtual checking accounts are similar to regular checking accounts that are also accessible online, except the virtual accounts have a few distinguishing features. With ING Direct's checking account, holders can transfer funds to pay bills online or instruct the bank to cut and mail a paper check to a named recipient. The system is intended "for people who don't need hand-holding" and whose online banking habits have created little need in their lives for paper checks or branch access, says Todd Sandler, ING Direct's head of deposit services.

Online banking: the early years

Virtual banking got its start in October 1995 with the launch of First Security Network Bank. Even now, only 3 to 4 percent of American households have virtual accounts, but the number of households that use them has surged with the rise in interest rates. From 2004 through 2006, while the Federal Reserve was steadily raising interest rates, the number of virtual-banking households jumped 61 percent, from 2.3 million to 3.7 million, according to Online Banking Report. Now Americans keep between $80 billion and $90 billion in virtual accounts, compared with about $3 trillion in retail accounts with balances under $100,000.

Safeguards a must

Despite growing acceptance of virtual accounts, safeguards remain crucial for reducing risk. The challenge for consumers is to recognize what the risks are and how to block them.

"In the online banking world, the risks are a little bit different" than in bricks-and-mortar banking, says Ron Teixeira, executive director of the National Cyber Security Alliance, a nonprofit cosponsored by federal agencies and private donors, including computer security companies. "Unfortunately, the risks are a little bit closer to home [in virtual banking] because they exist on your computer."

Example: a computer virus or spyware attack could result in the transmission of account information or passwords to a would-be thief anywhere in the world. Mr. Teixeira points to what happened to one man's online trading account during the summer of 2005. A fraudster, he says, used a virus to infect his computer (which didn't have up-to-date antivirus software), monitor his keystrokes, sell the man's stocks, and move funds to the fraudster's bank. When the man logged on to check his portfolio, his life's savings

of $174,000 was gone. He had no legal recourse, but the online brokerage opted to reimburse his account, Mr. Teixeira says. He suggests that a similar problem could happen to someone's Internet bank account. The lesson is to maintain up-to-date antivirus and antispyware software. Consumers also need to download free updates for their operating systems, such as those for Windows, to plug holes that violators may try to exploit.

Even with these defenses, vulnerabilities may persist. Both Teixeira and Colarik warn of so-called "man in the middle" attacks in which a perpetrator intercepts communication between a customer and an online bank and steals enough information to redirect funds. Teixeira says these violations are most likely to happen when a person accesses an account through an unsecured wireless platform, such as one offered at a cafe or hotel, where a thief might monitor a transaction surreptitiously.

Proper safeguards are necessary in part because the Federal Deposit Insurance Corp. (FDIC) doesn't insure against theft. Meanwhile, financial advisers say even Internet-savvy clients shouldn't close up their bricks-and-mortar accounts altogether.

"There are always things coming up where you want to go talk to your banker" in person, says Peter Cacioppo, a financial planner in Moraga, Calif. Example: a person who sells a car may want a trusted banker to verify whether a check is valid. And a virtual bank will probably take longer than a traditional bank to cash that check. The usual protocol at virtual banks is to endorse the check and drop it in the mail for depositing.