



Financial Crimes Enforcement Network Department of the Treasury

FinCEN would like to take the opportunity to advise you of two known fraudulent schemes:

1. The first scheme is one you may have already heard from your functional regulator, but in case you have not, Treasury's Assistant Secretary for Financial Institutions made the following public announcement last week:

Recently, many Americans have received a series of fraudulent e-mails, which direct recipients to websites where they are asked to verify sensitive personal information. The e-mails claim that the individual's personal information is necessary to assist in the fight against terrorism or for some other purpose supposedly required by law. These e-mails are purportedly sent from several government agencies or include content related to government agencies including the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the Securities Investor Protection Corporation and others. The websites to which the email recipients are directed are often very similar to, if not actual clones of official government sites.

The fraudulent e-mails are part of a scam known as "phishing." Phishing is the fraudulent scheme of sending an e-mail to a user falsely claiming to be a legitimate company. The email attempts to con the user into surrendering private information that could later be used for identity theft. The e-mail directs the user to visit a web-site where they are asked to update personal information, such as name, account and credit card numbers, passwords, social security numbers and other information. The Web site, however, is bogus and set up only to steal the user's information.

As part of the Treasury Department's efforts to fight identity theft, we want to assure Americans that federal financial agencies do not communicate with consumers by e-mail requesting important personal information such as your name, account numbers, date of birth, social security number.

Consumers can protect themselves from this latest identity theft scam by following these useful tips, which were developed by the Federal Trade Commission:

- If you get an email that warns you, with little or no notice, that an account of yours will be shut down unless you reconfirm your billing information, do not reply

or click on the link in the email. Instead, contact the company cited in the email using a telephone number or Web site address you know to be genuine.

- Avoid emailing personal and financial information. Before submitting financial information through a Web site, look for the "lock" icon on the browser's status bar. It signals that your information is secure during transmission.
- Review credit card and bank account statements as soon as you receive them to determine whether there are any unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.
- Report suspicious activity to the FTC. Send the actual spam to uce@ftc.gov. If you believe you've been scammed, file your complaint at www.ftc.gov, and then visit the FTC's Identity Theft Web site (www.ftc.gov/idtheft) to learn how to minimize your risk of damage from identity theft.

The Treasury and federal financial regulators are working hard to combat identity theft including the use of new tools in legislation recently signed by President Bush. But all consumers must take reasonable precautions in the use of their personal financial information in order to help prevent themselves from becoming victims of identity thieves.

2. The second scheme involves Fraudulent ANTI-TERRORIST STOP ORDER letters, purportedly sent by the Financial Crimes Enforcement Network (FinCEN). These letters are being sent to bank customers. Copies of these ANTI-TERRORIST letters have been received by FinCEN that notify consumers that mandatory fees, in amounts of approximately \$25,000, are required for the issuance of a ANTI-TERRORIST CERTIFICATE before transactions may continue to be conducted.

These letters were **NOT** sent by FinCEN and represent a fraudulent attempt to elicit funds from customers. Please see FinCEN's Website to see an example of one of these letters. Consumers should **NOT** provide any information nor send any funds, to any address as indicated in these letters. Further, consumers should **NOT** follow any instructions contained in these letters to access their accounts on-line.

Further, there are instances in which other letters are being circulated which claim that FinCEN is freezing assets and endorsing investment schemes. FinCEN does **NOT** have authority to freeze assets and does **NOT** endorse investment schemes.

FinCEN is working closely with law enforcement agencies to identify the source of these letters and disrupt these scams. Until this is accomplished, if consumers receive any letters such as these (Samples – [hyperlink](#)), or experience any similar attempts to obtain account information or funds, they are requested to notify FinCEN at webmaster@fincen.treas.gov