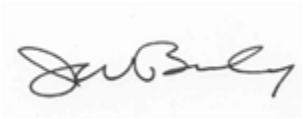
CPC CyberFlash

From the Director's Desk

The Officer Personnel Board (OPB) completed the commander and lieutenant commander selections. The Board recommendations will be forwarded to the Director, NOAA Corps who will review the recommendations on April 4, 2005 and forward those OPB recommendations to the Secretary.

The next Officer Assignment Board will convene on April 7, 2005. The billet list containing 299 priority billets will be released within the next three weeks. We are waiting for final comment from each Line Office (LO) Deputy Assistant Administrator. Once we receive their input we will describe the assignment and notification process. We anticipate the new process will enable officers to better track available assignments and allow for more timely notification. All officers shall coordinate their assignment preference with the appropriate LO liaison officer. The list of LO liaison officers will be published with the new billet list. Those officers who are proactive and communicate their preference to the LO liaison stand a better chance of receiving one of their assignment choices. Shore assignments are as critical as operational assignments and they will be filled by the best qualified officer at that time.

The assignment process is being stressed on all fronts which also stresses the officers. 280 officers cannot possibly fill 299 billets. Until we increase the size of the NOAA Corps the Officer Assignment Board (OAB) will have to make some difficult decisions. I thank you all for your hard work in the field and office, however, we remain a mobile uniform service and we are expected to go where NOAA requires us to go.



Captain Jonathan W. Bailey, NOAA
Director, Commissioned Personnel Center

PROTECTING YOUR IDENTITY

Some insurance companies recently began offering policyholders identity theft protection to help those who become victims recoup money spent on legal fees, lost wages and such

miscellaneous fees as mail and phone charges. Premiums vary, but typically range around $25 a year. Some policies have a deductible that the insured must pay before receiving benefits.

There's no sure method for protecting ourselves from identity theft, but we can minimize the risk by safeguarding personal information. One of the best ways to catch identity theft early is to order a credit report from each of the three major credit bureaus at least once a year.

TYPES OF FRAUD

- Bank fraud

- Bankruptcy fraud

- Criminal violations

- Fake driver's license

- Investment fraud

- Mail theft

- Passport fraud

- Phone fraud

- Social Security number theft and misuse

- Tax fraud

To protect yourself from fraud:

- Minimize the amount of identification you carry.

- Safeguard your Social Security number. Do not carry your Social Security card, and avoid using the number as an identifier.

- If your driver's license currently features your Social Security number, request an alternate number from the Department of Motor Vehicles.

- Don't put your Social Security number on checks.

- Be skeptical about revealing personal information. Know how it will be used and whether it will be shared with others. Ask if you can keep the information you share confidential.

- Know your billing cycles. Follow up with creditors if bills arrive late.

- Never give personal information to unsolicited telephone callers. For placement on a do-not-call list, go to www.the-dma.org/consumers/offtelephonelist.html. Information on state do-not-call lists is available at www.ftc.gov/donotcall.

- Cross-shred personal information before throwing it away. This includes charge receipts, copies of credit applications, insurance forms, bank checks and statements, expired charge cards and credit card offers.

- Remove your name from mailing lists for pre-approved credit lines. The credit industry's "prescreening opt-out" number is (888) 567-8688 or www.optoutprescreen.com.

- Close unused credit card or bank accounts.

- Place outgoing mail in post office collection boxes rather than in unsecured mail receptacles.

- Never leave receipts at bank machines, bank windows, gas pumps, etc. Save credit-card receipts to match against monthly bills.

- Sign all new credit cards upon receipt.

- Never put account numbers on post cards or on the outside of envelopes.

- Beware of mail or telephone solicitations disguised as promotions offering instant prizes or awards. They may be designed solely to obtain personal information or credit card numbers.

- Notify all banks, creditors and other businesses of your new address when moving.

- When submitting a change of address to the U.S. Post Office, follow up to be sure your address was indeed changed, so tenants at your old address do not receive your mail.

- Do not file your Department of Defense Form 214 (Military Discharge) with the county courthouse, since it then becomes public record.

- Do not display certificates or awards that list your Social Security number.

- Consider putting a fraud alert on your credit even if you have no suspicions of fraud. If you can't get instant credit, neither can a thief. (California currently allows consumers to place a credit freeze on their credit reports, but each credit bureau charges from $12 to $59.95 for those who are not victims of identity theft.)

PERSONAL SECURITY

To keep the personal information on your computer safe:

Update virus-protection software regularly.

Do not download files or click on hyperlinks sent by strangers.

Use a firewall program to stop uninvited guests from accessing your computer.

Use a secure browser to guard the security of your online transactions.

Try not to store financial information on any computer. If it is necessary, be sure to use a strong password with a combination of letters, numbers and symbols.

Do an Internet check on your name to see if personal information is easily available. Do not post personal information on the Internet.

When You're the Victim

"Unlike victims of other crimes, who generally are treated with respect and sympathy, identity-theft victims often find themselves having to prove that they're victims, too — not deadbeats trying to get out of paying bad debts. So how do you go about proving something you didn't do? Getting the right documents and getting them to the right people is key." from the Federal Trade Commission's "When Bad Things Happen to Your Good Name."

Clearing your name and records after fraud occurs can take considerable time and effort. Exactly which steps a victim should follow vary depending on individual circumstances and how the identity was misused. However, three basic actions should be taken in all cases:

Report identity theft to the fraud departments of each of the three major credit bureaus:

Equifax Credit Bureau

(800) 525-6285

Experian Information Solutions

(888) 397-3742

TransUnion Credit Bureau

(800) 680-7289

Request that a fraud alert be placed in each report, as well as a victim's statement asking that creditors call before opening new accounts or changing existing accounts. (Because fraud alerts are voluntary services provided by the credit bureaus, creditors do not have to consider them when granting credit. Most will, however, since they become responsible for damages if the account is fraudulent.) Also, order copies of your credit reports from each bureau, which

ordinarily cost about $9 but are free to victims of identity theft and individuals who have been denied credit.

Close all accounts that have been fraudulently accessed or opened. The contact for this is the security department of the agency that issued the credit card or the bank that holds the account that the thief accessed.

File a report with local police. Get copies for banks, creditors or others who need proof of the crime.

Additional steps include:

- Contact the Social Security Administration for a replacement if your Social Security card was lost or stolen, or for a new Social Security number in certain circumstances. Go to **www.ssa.gov** or call (800) 772-1213.

- File a complaint with the Federal Trade Commission's Identity Theft Division by calling (877) 438-4338 or logging onto **www.consumer.gov/idtheft**. The FTC is the federal clearinghouse for consumer complaints about identity theft. The FTC and other law-enforcement agencies use the information to track, investigate and prosecute identity thieves.

- Complete an ID theft affidavit at **www.consumer.gov/idtheft** if disputing fraudulent debts and accounts. This simplifies the process by limiting the number of forms that need to be filled out and helps financial companies in the investigation of fraud.

- Request new passwords and PIN numbers for accounts and credit/debit cards that have not been accessed.

- Contact your state's Department of Motor Vehicles to see if other licenses have been issued in your name. If so, request a new license number and fill out a complaint with the DMV.

- Organize your case by making a log of all contacts and keeping copies of all correspondence.

VICTIMS' RIGHTS

Some federal laws can help protect victims of identity theft, or help them undo some of the damage.

Under the **Fair Credit Reporting Act**:

- You have the right to receive your credit report. You are entitled to receive the report free of charge if your report is inaccurate because of fraud.

- You have the right to dispute errors in your credit report. The credit bureau and the company

that furnished the inaccurate information to the credit bureau must investigate the disputed information.

Under the **Fair Credit Billing Act** and **Truth-in-Lending Act**:

- If you report to the credit-card issuer that your credit card is lost or stolen, you cannot be held responsible for more than $50 of unauthorized charges.

- You have the right to dispute errors on your credit card bill. If you send a written notice to the credit card issuer within 60 days, it must investigate and either correct the error or explain why the bill is believed to be correct within two billing cycles or 90 days, whichever is less.

Under the **Fair Debt Collection Practices Act**:

- If a debt collector contacts you about a debt that you believe you do not owe, you have the right to file a dispute with the debt collector. If you do so in writing within 30 days of the collector's initial contact with you, the collector is required to stop all collection efforts until the debt is verified and the verification is sent to you.

Under the **Electronic Fund Transfer Act**:

- You have the right to dispute errors on your electronic fund-transfer account statements. If you send a written notice to the issuing financial institution within 60 days, it must investigate and either correct the error or explain why the account statement is believed to be correct, within 13 business days. In some cases, if the institution needs more time, it may take up to 45 days to complete the investigation.

Check with your state attorney general's office or the local police for additional protections or remedies under state laws.