Steel Valley Dolphins

August 2015

The official newsletter of the
USS Requin Base of the USSVI
Pittsburgh, Pennsylvania

USSVI Creed:

"To perpetuate the memory of our ship-mates who gave their lives in the pursuit of duties while serving their country. That their dedication, deeds, and supreme sacri-fice be a constant source of motivation to-ward greater accomplishments. Pledge loy-alty and patriotism to the United States of America and its Constitution."

Meetings held on the second Saturday of the month normally in Leetsdale at the VFW Post and quarterly meetings held around our membership area.

- **Make a difference, get to a meeting!**
-

---------- Pride Runs Deep ----------

Next meeting: NO MEETING T.HIS MONTH. Next Meeting at VFW Leetsdale Oct 12th @ 1230.

.

.

2015 USS Requin Base Officers

Base Commander	Hubert C. Dietrich	412-486-2635	hueyfromglenshaw@aol.com
1st Vice Commander	Joe Campisi	412-322-3201	jcampisi1@comcast.net
2nd Vice Commander	Ron Goron	724-626-1209	patron@zoominternet.net
Secretary	Jeff Simon	724-502-4505	jeffsimon@zoominternet.net
Treasurer	Lee M. Bookwalter	412-795-8337	booky143@verizon.net
Storekeeper	Joe Campisi	412-322-3201	jcampisi1@comcast.net
Chaplain	Carl Stigers	412-995-8028	carstenstigers@verizon.net
Past Base Commander	Joe Campisi	412-322-3201	jcampisi1@comcast.net
Newsletter Editor	Jack Sutherin	330-482-4175	jack.sutherin@comcast.net
Webmaster	Lee M. Bookwalter	412-795-8337	booky143@verizon.net
COB/Historian -	Clyde Porter, jr.	740-635-3179	candsporter@comcast.net

August

USS S 39 (SS 144)	August 16, 1942
USS POMPANO (SS 181)	August 29, 1943
USS FLIER (SS 250)	August 13, 1944
USS HARDER (SS 257)	August 24, 1944
USS BULLHEAD (SS 332)	August 6, 1945
USS COCHINO (SS 345)	August 26, 1949

Binnacle List

Bob and Carol Keller

. **Requin Base Meeting Minutes**
August 08, 2015
Leetsdale, PA

Base Commander Huey Dietrich called the meeting to order.
Attendees: Martin & Kyle Abel, Mike Allen, Greg & Maggie Bayne, Lee & Patsy Bookwalter, Clair & Nancy Bouts, Don Bright, Joe Campisi, Huey & Edie Dietrich, Aaron & Sandy Ellis, Rick& Judy Elster, Peter Foster, Major Galloway, Gerry & Linda Gaylor, Richard & Beverly Geyer, Ric & Joan Guntag, Lou & Alex Hamil, James Messer, Frank Nicotra, Bob & Linda Renninger,J eff Sammel, Jeff & Eileen Simon, Bob & Dorothy Stahl, George Stass, John & Lois Stewart, Carl Stigers, Jack & Jenny Sutherin, and guest Eric Greenwald.
Base Commander Huey Dietrich gave the quote of the day: "Nothing needs reforming so much as other people's habits"
Requin History: August 24, 1944 keel laid at Portsmouth Naval Shipyard. August 14, 1945 two weeks after her arrival and three days before starting her first war patrol, WWII ended and the Requin was recalled and ordered back to the Atlantic. August 1, 1952 Requin was back in European waters, during September she visited the United Kingdom, then in October the submarine transited the Straits Of Gibraltar for regular 6th Fleet duty. August 15, 1959 upon her conversion to fleet snorkel configuration, the Requin was given hull classification SS 481 and rejoined Subron 6 in Norfolk VA for operations as a normal attack submarine, a role she retained until her decommissioning. August 7, 1990 Requin left International Ship Repair in Tampa FL under tow to Baton Rouge LA. August 11, 1990 Requin was lifted onto barges and began her ride up the Mississippi River and Ohio River to Pittsburgh PA.
Base Commander Huey Dietrich: Let us at this time, with a moment of silent prayer, remember our Shipmates who made the supreme sacrifice that we may gather here in Peace. We dedicate this meeting to our Shipmates on Eternal Patrol, to perpetuate their memories in our lives and to honor our Shipmates on active duty in the service of the first line of defense of our Nation.
Boats Lost:

USS BULLHEAD (SS 332)	August 6, 1945
USS FLIER (SS 250)	August 13, 1944
USS S 39 (SS 144)	August 16, 1942
USS HARDER (SS 257)	August 24, 1944
USS COCHINO (SS 345)	August 26, 1949

We also wish to remember our shipmates of the Requin Base: Neal Sever, Frank Gogul, John Irons, and Louis Kleinlein, Ed Yoder, Joe Brenkus, Steve Kossler. Let us also remember the brave submariners who died performing their duties aboard submarines, some individually and some in groups, but where the submarine itself was not lost.
Chaplain Carl Stigers gave the Invocation.
Base Secretary Jeff Simon led the Base in the Pledge of Allegiance.
Members introduced themselves and the boats they qualified on.
Base Secretary Jeff Simon reported that Minutes of the last meeting were published in the SVD.
Treasurer Lee Bookwalter's report was presented and approved by the members present.
Other Reports:
Eternal Patrol Joe Brenkus, Steve Kossler and Ed Yoder
Binnacle List includes Mat Holzer, Bob Keller, Carol Keller, Mike Markel, Clyde Porter.
Membership stands at 214 making Requin the sixth largest USSVI base.
Eagle Scouts presentations are ongoing and members are encouraged to participate.
On Labor Day, Shipmate Bob Bitner is bringing 20 kids and families from Children's Hospital to the Requin for the Kap(SS)4Kid (SS) program.
Memorials And Ceremonies:
Nothing planned
Old Business:
Efforts to name the new north shore subway tunnel in Pittsburgh for the USSVI were unsuccessful.
No September meeting due to the convention.
A visual walkthrough of the USS Requin is being prepared by Shipmate Lou Hamill, pending approval of the Science Center, and will be posted on the new USS Requin website.
Additional caps, longevity pins and other supplies have been ordered.
New Business:
Busy with convention and eternal patrol services.
For The Good Of The Order:
Eric Greenwald explained the mission of his reserve unit that will be assisting us during the convention.
Convention News:
Convention bags have been ordered
A total of 42 Pirates baseball tickets were sold.
Convention magazine will go to the printer soon.
Guest Speakers:

Men's Luncheon – Dave Campbell
Banquet – Admiral Hilarides USN
Holland Club – Joe Buff
Women's Luncheon – TBD
Volunteers are needed to help set up.
Contact Huey Dietrich to purchase raffle tickets for a quilt made by Carol Keller.
Chaplain Carl Stigers gave the Benediction and blessing of today's meal.
Adjournment: The meeting was adjourned.
Next meeting: Leetsdale, PA VFW at 1230 hours on October 10, 2015.

COMMANDERS COLUMN:

The August meeting was a great success! Two new members participated in their first meeting of the Requin base and the shipmates were very excited that they joined. Major Galloway walked in and surprised us. He belongs to the Arkansas Base and joined us as a duel member. Also ETCS Eric Greenwald from the Navy Reserves, not only joined the base but gave us a detail description of his duties when he is on assignment. He has volunteered his unit to assist us where ever we may need them during the convention.

DUES - 2016

Our annual dues collection process will be starting right after the convention. The schedule for dues collection will be as follows:

SEPTEMBER - Base Officers & Committees
OCTOBER - Base Members that live in Pennsylvania
NOVEMBER - Base Members that live outside of Pennsylvania
DECEMBER - New Members that joined in 2014

The USSVI has voted to increase dues for 2016, from $20.00 to $25.00. But if you pay your dues before December 31, it

will still be $20.00 for 2016. The Requin Base dues is remaining at $10.00 per year. So our total dues will be $30.00 if paid before the end of the year. **WHEN YOU RECEIVE YOUR DUES PACKET, PLEASE DO NOT SET IT ASIDE.**

Also included with your dues packet will be your 2016 USSVI calendar. If anyone does not want to receive the calendar, please let me know, and we will not send it to you. This is a big undertaking and unfortunately mistakes will be made. If you receive it in error, please return it and then deduct the postage from your dues check. The base uses the calendars for a fund raiser to cover our base expenses. The cost of the calendars from the USSVI has also increased by $1.00.

Here is the anticipated dues packet cost:
National Dues ----------$20.00 (if paid before Dec 31) $25.00 after.
Base Dues---------- 10.00
Calendar---------- 8.00 -($10.95 from National Storekeeper)
Postage---------- 2.25
$40.00 - The base will absorb the extra .25c
To save postage, pick up your calendar during the convention or at a base meeting before your schedule dues month.

CONVENTION

The convention committee is working extremely hard and they are fine tuning all the plans in place. If anyone wants to volunteer their services and help us with all the activities, please e-mail me or give me a call - 412-486-2635. Everything is shaping up and hopefully everyone will have a great time. We will have several raffles throughout the week and if you won't be able to make the convention, you can always buy some tickets. E-mail me if your interested.

HANGING QUILT - made by Carol Keller, who suffered two strokes, still wanted to keep her promise to us and did a beautiful job.
$2.00 apiece or 3 for $5.00

PA SCRATCH
LOTTERY TICKETS - there is $200.00 worth of Pa lottery tickets- **6 tickets for $5.00 or 13 tickets for $10.00**
CHINESE - There are 20 beautiful baskets donated by base members/spouses.
- **25 tickets for $10.00**

Flat Screen TV - The base is purchasing the T.V. to be used for the Kap(SS) 4 Kid(SS) program at the convention and then raffled off. **6 tickets for $5.00**

50/50 - **6 tickets for $5.00**

NEW MEMBERS

MAJOR GALLOWAY - qualified on the USS ARCHERFISH-SSN678 in 1972 as a FTG2(SS). He left the navy in 1976. Major lives in Scottsdale, Pa with his first mate Loretta. Please e-mail Major and welcome him aboard - majdyland@gmail.com

ERIC GREENWALD - qualified on the USS OHIO-SSBN/SSGN726 in 2003 as a ET1(SS). He left the navy in 2002. Eric is currently a ETCS(SS) in the navy reserves in Pittsburgh. Eric lives in Monroeville, Pa., with his first mate Danielle. Please e-mail Eric and welcome him aboard - ericjgreenwald@gmail.com

EDWARD PERLOWITZ - qualified on the USS JACKSONVILLE-SSN699 in 1986 as a MM2(SS). He left the navy in 1989. Ed lives in Wexford, Pa . Please e-mail Edward and welcome him aboard - eperlowitz@aol.com

Membership is standing at 216 members, which puts us at the sixth largest base in the USSVI. If we put on a big push at the convention and the rest of the year, we could become the fifth largest.

BIRTHDAYS
Al Breamer - 8/10/33
Don Bright - 8/01/52
Dennis Cantwell - 8/29/47
Aaron Ellis - 8/21/36
Robert Emery - 8/16/53
Fred Hayes - 8/16/53
Frank Indo - 8/18/47
Bob Keller - 8/03/41
Al Murman - 8/16/37

ANNIVERSARIES
Bill & Madeleine Beadle 8/29
Aaron & Sandy Ellis 8/1
Henry & Agnes Franz 8/13
Herb & Evelyn Hollingsworth 8/30
Mat & Margaret Holzer 8/29
Bob & Carol Keller 8/11
Merlin & Judy Larson 8/15
Robert & Rita Lindsey 8/18
Ron & Pamela Lucas 8/15

Robert Stahl - 8/10/23
Mark Winters - 8/31/54

FIRST MATES

Judy Edwards - 8/19
Carmella Markel - 8/27
Karen McGee - 8/10
Francis Osborn - 8/24
Marilyn Regits 8/07
Dottie Sigler 8/09
Sandra Staas - 8/16
Louis Stewart - 8/07

Ed & Dot Paul 8/19
George & Sandy Staas 8/24
Ralph & Trudith Strode 8/09
Mark & Brenda Winters 8/02
Garry & Susan Ireland 8/74
Bob & Debra MacPherson 8/30

US Navy Sidelines 3 Newest Subs

Chris Cavas, Defense News, Aug 5

WASHINGTON — The US Navy has restricted the operations of its three newest submarines — including one placed in commission just last Saturday — pending inspections and repairs to a key steam plant component.

At issue are problems found with elbows in 10-inch pipes that funnel steam from the reactor plant to the propulsion turbines. Elbows are installed in piping to get around corners and other obstructions.

The problems, said a senior Navy official, were detected earlier this year, prompting a civil investigative demand leading to an investigation begun in April. A fleet message restricting operations of the three submarines was sent Aug. 5, and congressional authorities were notified the same day.

Rory O'Connor, a spokesman for the Naval Sea Systems Command (NAVSEA) in Washington, said the problems affect the submarines Minnesota, North Dakota and John Warner. He described the situation late Wednesday in a statement:

"As part of an ongoing investigation into a quality control issue with a supplier, General Dynamics Electric Boat (GDEB) determined that three steam pipe elbows supplied by the vendor in question required additional testing and repair due to unauthorized and undocumented weld repairs having been performed on these elbows.

"GDEB along with Huntington Ingalls Industries-Newport News Shipbuilding (HII-NNS) are performing additional inspections to bound the issue. Currently, USS Minnesota (SSN 783), USS North Dakota (SSN 784), and USS John Warner (SSN 785) are impacted.

"The Navy is committed to ensuring the safety of its crews and ships. High quality standards for submarine components are an important part of the overall effort to ensure safety."

The problem, said the senior Navy official, "is not a safety concern in terms of what's involved right now. Basically it's being prudent in looking into it." The concern, the official added, is "long-term wear-and-tear."

The Navy, said the senior Navy official, is developing a more detailed inspection plan before certifying affected submarines for further operations.

It is not clear what prompted the investigation, but it was apparently begun at the behest of Electric Boat.

Construction of Virginia-class submarines is split evenly between Electric Boat in Connecticut and Rhode Island, and Newport News Shipbuilding in Virginia. The yards, however, do not supply pipe elbows.

According to an official source, the defective elbows are manufactured by Nuflo, a Jacksonville, Florida-based company that, according to its website, "manufactures piping solutions for every aspect of industry." The company, "has been qualified for the most critical standards of quality and inspection certifications," the site continued.

According to the senior Navy official, the Nuflo pipe elbows initially failed magnetic test inspections that showed "minor surface indications," then successfully passed ultrasonic test inspections after minor repairs.

Further testing by Electric Boat using acid etch inspections, however, showed that "unauthorized and undocumented weld repairs had been performed by the vendor on these elbows.

Nuflo had not responded to phone messages or emails from a reporter before this story was published.

According to the senior Navy official, the suspect elbows are not believed to have been installed on submarines built before the Minnesota, which was commissioned in September 2013. Ten elbows were installed on subs now in service — one on the Minnesota, six on the North Dakota, three on the John Warner. Another 40 elbows were installed on still-incomplete submarines or are in stock.

In late July, the Minnesota was to have completed its post-shakedown availability (PSA), a major, post-delivery overhaul that fixes problems found during a sub's initial service period, provides system updates and puts on finishing touches wherever needed. But the submarine is still at Electric Boat's shipyard in Groton, Connecticut, and its "maintenance availability has been extended to support the evaluation," O'Connor said.

The North Dakota, commissioned in October, is at Submarine Base New London, just upriver from Groton, and is expected to move to the shipyard in a few weeks to begin its PSA, during which the elbow problems will be addressed. The submarine returned to New London on July 20 from a seven-week mission.

The John Warner, which was officially placed in service Saturday in a ceremony at Norfolk attended by her namesake and top Navy officials, has had its operations "restricted until the investigation is complete and the issue has been adjudicated," O'Connor said.

Another submarine, the Illinois, is expected to be floated off for the first time in a few days at Groton. Any problems with the ship, O'Connor said, "will be taken care of in construction."

Sleep Apnea Update 05 ► OSA Causes, Risks, and Treatment

We all know what it is like to feel tired after a sleepless night because of things like noise, worries or stress. But what if you do actually get enough sleep and still feel absolutely beat the next morning? This is normal for many people with obstructive sleep apnea (OSA): They do not get enough air while they are sleeping (but do not usually notice this), have breathing pauses, and feel very sleepy during the day. In the long term, this increases their risk of developing other illnesses and can have a huge effect on their quality of life. People who have obstructive sleep apnea usually snore very loudly and regularly have phases of shallow breathing (hypopnea) and breathing pauses (apnea) that last longer than ten seconds while they are sleeping. Snoring itself is harmless; it is only classified as sleep apnea if you have breathing pauses too. The following symptoms may also be signs of sleep apnea:
Night sweats and frequent urination

- Waking up suddenly, sometimes with a racing heartbeat and shortness of breath
- Dry mouth when waking up
- Headaches in the morning
- Exhaustion during the day

Poor concentration

Causes and risk factors. Sleep apnea is caused by the muscles of the upper respiratory system relaxing. Your throat then becomes narrow or even completely blocked, which leads to loud snoring noises when you breathe in and out. As a result, your body does not get enough oxygen. Your pulse and blood pressure fall too. The part of your brain responsible for breathing sets off an alarm and triggers a wake-up call, causing you to wake up briefly, usually without realizing it. This interrupts your natural sleep pattern, your heart starts beating faster and your blood pressure rises. If this keeps happening throughout the night, it may prevent you from entering deep sleep, which is what is needed to get restful sleep.

Being very overweight and having unusual features in the mouth and throat area are common causes. These unusual features include enlarged tonsils, a small lower jaw, the position of the tongue and a small soft palate. Nasal breathing is sometimes obstructed too. Sleeping on your back can make snoring and breathing difficulties more likely, but is rarely the sole cause. Drinking too much alcohol and taking sleeping pills or sedatives relaxes the throat muscles and can make sleep apnea worse. The likelihood of developing obstructive sleep apnea increases constantly after the age of 45. It is estimated that 4 out of every 100 middle-aged men and 2 out of every 100 middle-aged women have obstructive sleep apnea that causes symptoms.

Effects. Severe sleep apnea makes you feel constantly worn out and tired. Not getting enough restful sleep can have longer-term effects on your mood too. If you generally do not feel as well as people who usually get a good night's sleep, you are also more likely to become depressed. High blood pressure (hypertension) and other cardiovascular diseases are more common in people who have sleep apnea. They are more likely to have a heart attack, a stroke or heart rhythm problems (arrhythmias) as a result. Breathing pauses do not always pose a problem or health risk. If they only occur now and then, are short, and do not cause tiredness during the day, there is usually no reason to worry. Yet it may be a good idea to keep an eye on any breathing difficulties and see a doctor if they cause more long-term problems.

Diagnosis. If it is thought you might have obstructive sleep apnea, your doctor will first ask you about your symptoms and lifestyle habits. This is usually followed by a general physical examination. You may be given a portable monitoring device which can be used when you are asleep to record things like your breathing, heart rate, blood oxygen levels, snoring, and body position. If there are any irregularities, further tests in a sleep laboratory may be a good idea. Sleep laboratories have bedrooms that can be used for one or more nights. Here your sleep is monitored using different recording devices and a video camera. As well as recording your breathing, pulse, blood pressure and blood oxygen levels, they also record your brainwaves, and your eye and leg movements during sleep. Using the recorded data, the different sleep phases can be analyzed to see how long and how well you slept, and whether you spent enough time in deep sleep and dreaming. In people with sleep apnea, the machines can record how often breathing pauses occur, how long they last, during which sleep phases they occur, and the patient's sleeping position at the time. It is also possible to tell how they affect the cardiovascular system and blood oxygen levels.

Treatment. If you are very overweight, losing weight can help improve sleep apnea. There are also many treatment options that aim to relieve sleep apnea. These include machines that support breathing during the night, surgery, and special aids such as mouth guards. Some of these treatments have been scientifically proven to help people with sleep apnea. Medication is currently not used for the treatment of sleep apnea. There is no scientific evidence that the available medications work. CPAP therapy is the most effective way to relieve obstructive sleep apnea, but it is difficult to get used to. Not everyone wants to wear a breathing mask every night.

Patient education programs can help you get to grips with CPAP therapy. Joining a self-help group and talking with other people who have sleep apnea can help too. The most important thing is to be patient and get the support you need if you have any problems. If you manage to make breathing therapy a part of your daily routine, it can really improve your quality of life.

CPAP stands for “continuous positive airway pressure.” In this treatment approach, air is taken from the immediate surroundings and blown into your airways at night using low pressure. While you sleep, you wear a breathing mask that is connected to a machine called a respirator. The pressure keeps the upper airways open. People who use this machine have fewer breathing pauses, or even none at all. This can noticeably improve the symptoms such as tiredness during the day. Common side effects include a dry throat and an irritated, sometimes blocked nose.

Dental Hygiene ► Don't Believe All of the Advertising Hype

According to this article written by Dr. Eric Spieler - a practicing dentist in Philadelphia, PA - Just about everyone wastes money when it comes to purchasing and using toothpaste. We usually use two to three times as much toothpaste as is necessary. Some dentists advise that a pea size drop of toothpaste is sufficient to clean teeth and gums. Others suggest that you use enough toothpaste to just cover the toothbrush bristles with a thin flat layer of toothpaste. Both amounts, however, are far less than what most people use. It seems that over our lifetimes we have been conditioned into thinking that the amounts of toothpaste we see in ads is the amount needed for good oral health.

We also tend to waste money when we buy expensive toothpastes containing ingredients which we are led to believe will result in cleaner teeth. Often, however, these ingredients don't result in cleaner teeth but just the sensation of cleaner teeth. Baking soda found in many expensive toothpastes is a prime example. Although it may make our mouth feel clean, a Journal of the American Dental Association study revealed that baking soda is no more effective in cleaning teeth than normal toothpaste. Another much hyped toothpaste ingredient is peroxide. Peroxide creates small bubbles in the mouth which massage the gums providing a cleaning sensation. While the bubbling action created by peroxide may provide a cleaning sensation it does little to actually clean teeth and gums. The bottom line is that when it comes to toothpaste just about any toothpaste that contains fluoride will do a good job in cleaning our teeth and gums.

Another marketing feat has been performed by our friends in the mouthwash industry. Dentists and hygienists have often questioned the claims of mouthwashes to eliminate bad breath and reduce plaque formation. Bad breath is caused by bacteria on tooth surfaces which break down food particles left after we eat. One of the by- products of this breakdown is foul smelling sulfur particles. Most mouthwashes do not eliminate bad breath but simply mask odor - usually only very temporarily. In this respect, most conventional mouthwashes are a waste of money. A new breed of mouthwashes, however, actually helps to eliminate bad breath. Containing the active ingredient chlorine dioxide, these mouthwashes actually destroy foul smelling sulfur compounds. Consequently mouthwashes containing chlorine dioxide may well be worth the money.

What about the ability of mouthwashes to reduce plaque? - Plaque is an accumulation of bacteria, small particles, proteins, and mucous. When not properly removed by brushing and flossing, the bacteria in plaque can multiply and create harmful toxins which attack gum tissue. This is known as gingivitis. Unchecked gingivitis can lead to periodontal disease which is costly and often painful to treat. Unfortunately, clinical studies have shown that mouthwashes do very little to kill bacteria. There is one exception however. Listerine is the only over the counter mouthwash to have been clinically proven to kill bacteria which cause plaque and gingivitis. In this respect, the product more than lives up to its advertising hype.

Did you know that expensive mints and breath sprays may also be a waste of money? These help eliminate bad breath by stimulating saliva production! When it comes to reducing bad breath it seems that saliva is our friend. Saliva helps dissolve smelly sulfur particles and washes away bacteria and food particles. (One reason for bad morning breath is the lack of saliva production during sleep) Anything that stimulates saliva production can therefore help combat bad breath. Instead of taking a breath mint try a drink of water or eating, both of which stimulate saliva production.

What's one of the best dental products you can buy? Besides fluoride toothpaste and a good toothbrush one of the best dental buys is dental floss. Relatively inexpensive, the use of dental floss can save hundreds to thousands of dollars in future dental costs. You see by brushing we rid the mouth of bacteria reducing the risk of gingivitis and periodontal disease. We also help ensure that our breath remains fresh smelling. If we only brush however, we miss the bacteria that reside on tooth surfaces that the toothbrush cannot

reach. These include the spaces in between teeth. Here bacteria will be allowed to grow uninhibited leading to plaque formation, gingivitis, periodontal disease, and tooth decay. These conditions can be very costly to treat. Flossing removes bacteria in areas the toothbrush cannot reach.

In conclusion don't believe all of the advertising hype. For healthy people, when it comes to good home dental care a simple fluoride toothpaste, a good soft bristle toothbrush, and regular use of dental floss will work wonders. [Source: The Dollar Stretcher | Eric Spieler | August 2015 ++]

IRAs Update 02 ► What Happens if Hacked

Other than perhaps your home equity, your investment accounts, including your 401(k) and other retirement accounts, are likely where most of your net worth resides. What happens if these accounts are hacked? You'd assume you wouldn't suffer a loss if someone fraudulently withdrew money from any type of account, whether bank, brokerage, credit card or retirement plan. But that's not the case. While there are laws that limit your losses if your credit or debit cards are compromised, there aren't specific laws protecting you from cybertheft-related losses in your brokerage account.

If hackers gain access to your brokerage account by hacking into your firm's servers, odds are good you'd be reimbursed. But if the cybertheft occurs on a more personal level, the outcome could be a lot worse. Say you get an email from your brokerage firm stating your monthly statement is ready for review. You click the link within the email, which takes you to the login page of your brokerage website. You enter your username and password, check your balances and go on with your day. But the email you responded to was fake. The website you were on looked like the login page of your brokerage account, but the site was a decoy designed to separate you from your login credentials. Now that they have your username and password, the crooks are in a position to empty your account. Does the brokerage firm have to reimburse you? No. They could simply claim that you're supposed to keep your login information secret and you didn't. The fact you responded to a legitimate-looking email isn't their problem. There's no law requiring them to reimburse you.

A few months ago, the SEC examined 57 registered broker-dealers and 49 registered investment advisers. According to their report: *Written policies and procedures generally do not address how firms determine whether they are responsible for client losses associated with cyber incidents. The policies and procedures of only a small number of the broker-dealers (30 percent) and the advisers (13 percent) contain such provisions, and even fewer of the broker-dealers (15 percent) and the advisers (9 percent) offered security guarantees to protect their clients against cyber-related losses.*

What happens if you get ripped off? If you've got money with a brokerage or investment firm, step one is to see what kind of protection your broker offers in cases of cyber breach. Here are links to fraud policies of three popular investment firms:
Vanguard's online fraud policy
Charles Schwab Security Guarantee
Fidelity Customer Protection Guarantee

As an example, here's the language Vanguard uses to introduce its policy: *Our commitment regarding online security is simple. If assets are taken from your account in an unauthorized online transaction on Vanguard.com® — and you've followed the steps described in the Your responsibilities section below — we will reimburse the assets taken from your account in the unauthorized transaction.* Sounds good. But what exactly are your responsibilities? Here are the highlights.

Review your accounts regularly.

Protect your Vanguard.com user name, password, and other account-related information.

Protect your computer.

Do not reply to e-mail requests for personal or financial information.

Cooperate with us and stay informed.

You can review the details under each of these headings on their policy page, but you get the idea. Unlike with a credit card, when it comes to investment accounts, you're not off the hook simply because someone hacked your information. You're responsible for keeping your account safe. Also worth noting is the fine print at the bottom of the policy page, which reads in part: *This protection does not apply to unauthorized activity caused in whole or in part by your fraudulent, intentional, or negligent acts or omissions, including activity by a person whom you have intentionally or negligently permitted to transact in your account, or to whom you have intentionally or negligently given access to security information relating to your account. This protection does not apply to unauthorized account activity or account access by an employer or plan sponsor representative who is authorized to access your account but is acting outside the scope of his or her authority.*

In other words, if you negligently allow someone to obtain your login information, the guarantee doesn't apply. (And who decides

what constitutes negligence? They do.) Nor, in the case of retirement accounts, does the guarantee apply if your employer or plan sponsor rips you off; something completely beyond your control. This lack of investment firm accountability is frightening, particularly in light of the potential money involved and the amount of online fraud that's occurring these days. The SEC put out an investor bulletin called Protecting Your Online Brokerage Accounts from Fraud that every investor should read. Here are the steps they suggest:

Pick a strong password, keep it secure, and change it regularly.

Use two-step verification, if available.

Use different passwords for different online accounts.

Avoid using public computers to access your online brokerage account.

Use caution with wireless connections.

Be extra careful before clicking on links sent to you.

Secure your mobile devices.

Regularly check your account statements and trade confirmations.

Click the link above to get more detail on their suggestions. Other sites to review include the SEC's Online Brokerage Accounts: What You Can Do to Safeguard Your Money and Your Personal Information, FINRA's Protect Your Online Brokerage Account: Safety Should Come First When Logging In and Out and the FTC's Tips for Using Public Wi-Fi Networks. Bottom line? Your investment accounts don't carry the same legal protections as your credit cards, and they're likely to contain a heck of a lot more money. Take the necessary precautions. [Source: MoneyTalksNews | Stacy Johnson | July 28, 2015 ++]

Identity Theft Protection ► Does it Really work?

Perhaps your data was compromised in a high-profile data breach at a health insurance company, or you were one of the unlucky victims of the Target or Best Buy hacks. Or maybe you got a letter in June from the Office of Personnel Management, years after you quit your last government job. If you landed in any of these unfortunate categories—and it's not unlikely that you did, given the sheer scale of some of these data breaches—your consolation prize probably looked something like a free termed subscription to a credit-monitoring and identity-fraud-protection service. The government in June paid about $20 million to offer the 4.2 million current and former federal employees affected by a data breach with 18 months of protection services from CSID. According to CSID President Joe Ross, almost a million people took the government up on the offer—an astronomical uptake rate compared to average enrollment rates after most private-sector breaches.

But for a service that is often presented as a remedy for breaches that expose sensitive information, credit monitoring and identity-theft protection is far from a panacea. The programs CSID and its competitors provide range from simple credit monitoring to robust identity-theft protection. The suite of services the government purchased for OPM hack victims in June was "the whole kit and caboodle," according to a spokesman for CSID, and included public-records and loan monitoring, a program that monitors shady corners of the Web to see if clients' personal information is being traded or sold, and $1 million in insurance from damages in the event of identity fraud.

Eric Warbasse, senior director of financial services and breach response at LifeLock, touted the utility of fraud-protection programs in an interview earlier this month. "Enrolling in a service or services that include remediation as a backup in the event that somebody is impacted—has their taxes filed fraudulently, for example, something that would never show on a credit report—is a wise decision regardless of whether or not you're part of the OPM breach," Warbasse said, referring to programs that help victims restore the integrity of their identities after an incident of fraud. But security experts and the government have questioned the utility and security of these services, suggesting that signing up for a protection program is not enough to safeguard customers' identity.

The Federal Trade Commission last week took legal action against LifeLock over data-security practices the agency said do not adequately protect consumer information. The FTC alleged that LifeLock violated the terms of a 2010 settlement, in which the company paid $12 million over claims that it was falsely advertising the security and robustness of its service. Concerns about the company's practices were raised also by a whistle-blowing executive last year and by Experian, a credit-reporting agency, in 2008. Costis

Toregas, associate director of the Cyber Security Policy and Research Institute at George Washington University, said the allegations of security shortcomings are not new. "It doesn't surprise me, because we know that companies whose job it is to secure data are themselves vulnerable," said Toregas. "Am I shocked and surprised that I found gambling going on in the back room? No," Toregas continued. "Everything is hackable. They should be very, very careful of their promises."

LifeLock says it disagrees with the FTC's decision and will fight the new allegations in court. "Based on the evidence, we do not believe that anything the FTC is alleging has resulted in any member's data being taken," the company said in a statement. Just one day before the FTC's charges were announced, lawmakers from the House Energy and Commerce Committee sent a letter asking the Government Accountability Office to study the "usefulness and adequacy" of offering ID-theft-protection services to hack victims. The bipartisan group who signed the letter asked the GAO to answer questions about taxpayer cost and the state of service providers' security standards. House Minority Whip Steny Hoyer said Monday that identity-theft monitoring may never be enough to protect individuals who lost sensitive personal info. The 21.5 million victims of an OPM data breach announced earlier this month had their names, addresses, and Social Security numbers compromised, and 1.1 million individuals had their fingerprints stolen. "There may be some things we can't compensate for," Hoyer said.

That said, victims of data breaches who are offered months or years of free identity-theft-protection services should take advantage of it, said Toregas. "Never look at a gift horse in the mouth," he said. "For sure, accept it. But do not think that that is adequate." Toregas advises breach victims to learn about cybersecurity practices, change their online lifestyles to manage risk, and always operate under the assumption that their personal information has been stolen at least once. "Breaches have nothing to do with computers," he said. "They have everything to with your life. They have everything to with your career, with your credit, with your happiness, with your ability to get on an airplane and not to be arrested for a different identity, and so on." [Source: National Journal | Kaveh Waddell | July 28, 2015 ++]

This Is The U.S. Navy's Most Secretive Submarine

David Axe, The Week, Aug 20

No, the U.S. Navy is probably not using a multi-billion dollar submarine to listen in on your phone calls and emails on behalf of the National Security Agency.

But it could.

A long line of secretive Navy spy submarines, most recently a nuclear-powered behemoth named USS Jimmy Carter, have for decades infiltrated remote waters to gather intelligence on rival states' militaries, insurgents, and terrorists on behalf of the NSA and other agencies using a range of sophisticated devices, including special equipment for tapping undersea communications cables.

Before NSA whistleblower Edward Snowden revealed the agency's phone and internet monitoring programs targeting U.S. and European citizens, the mainstream press paid little attention to the elusive, subsurface warship. But following Snowden's disclosures in 2013, several publications including The Huffington Post and the German Der Spiegel speculated that the Jimmy Carter was aiding the NSA's surveillance of citizens' communications in the U.S. and Europe.

"It seems this same submarine," The Huffington Post claimed, "was pressed into service to spy on Europe."

The modified Seawolf-class sub, built by General Dynamics Electric Boat in Connecticut between 1998 and 2004, is almost certainly able to tap the undersea communication cables that carry much of the world's phone and internet traffic. But just because the warship can tap cables doesn't mean it routinely does.

At the Navy's request, Electric Boat inserted an extension in the middle of Jimmy Carter's hull that added 100 feet to its standard 350-foot length — plus nearly $1 billion to the baseline $2 billion price tag. Commander Christy Hagen, a Navy spokesperson, declined to comment on the warship's modifications.

But Owen Cote, a submarine expert at the Massachusetts Institute of Technology, said Jimmy Carter's hull extension most likely contains a "moon well" — a floodable chamber to allow divers, robots, and machinery to move between the sub's interior and the water, retrieving objects off the seafloor or carrying monitoring devices and other surveillance equipment.

With this, Jimmy Carter could, in theory, tap seafloor fiber-optic cables, said Norman Polmar, a naval analyst and author who has advised the government on submarine-building strategy. "You hook something on to the cable," Polmar said, "and come back in a month and remove the tape and take it back and analyze it."

But underwater wiretapping is probably unnecessary. "I don't think you need to use Jimmy Carter to do that," Cote said. "It would be a waste of that asset."

It's far easier for the NSA to monitor Americans' communications on land, Cote pointed out in an interview, with the consent of phone and internet providers.

But it wasn't long ago that Jimmy Carter's predecessor subs were involved in undersea eavesdropping — against America's Cold War rivals. That espionage took place during a technologically simpler time, when Washington had fewer ways of listening in on communications.

"Fifty, 60 years ago, this was best method of collecting certain intelligence," Polmar says of eavesdropping submarines. Before Jimmy Carter, there were the modified submarines Halibut, Seawolf, and Parche, fitted with special equipment for monitoring and accessing objects on the seafloor, including communications cables. Parche, the last of the old breed, was decommissioned in 2004, just as Jimmy Carter was nearing completion.

The subs' secret missions, the subjects of repeated investigations by high-profile reporters including Seymour Hersh in The New York Times, were practically the stuff of fiction.

In 1968, the Pentagon deployed Halibut to the Pacific to search for the wreckage of a sunken Soviet submarine that would later be partially recovered by a CIA team aboard a purpose-built salvage ship. Trailing a four-mile long cable rigged with cameras, Halibut found the Soviet vessel in 16,000 feet of water after just three weeks.

In the 1970s, Seawolf and Parche took risky missions penetrating the Soviet navy's main North Atlantic bastions to tap military communication cables. The two subs sailed under the Arctic at speeds of just a few miles per hour to avoid icebergs, dodging Soviet vessels and excitable seals and walruses that might betray the U.S. ships' locations.

The special subs placed on the cables clamp-like devices that recorded passing signals, giving Washington valuable insight into Soviet naval activities. In 1980, a former NSA employee named Ronald Pelton betrayed the subs' operations to the Soviets in exchange for around $35,000. Pelton was arrested in 1986, tried and convicted. He remains in federal prison.

The Soviets' discovery of the undersea wiretap alerted America's rivals, making such missions much more difficult. "People are now aware that that's a technological capability that we have — and that puts them on guard," Polmar says.

The disclosure, and new technology advances, has led to an apparent shift in the spy subs' tactics. When North Korea shelled a South Korean island base in 2010, Jimmy Carter reportedly surfaced nearby and launched a small, quiet drone spy plane to photograph the damage. Since then Jimmy Carter has undoubtedly stayed busy performing other surveillance missions and, in 2013, entered a roughly yearlong period of maintenance at a shipyard in Washington State.

Now that the submarine has returned to the fleet, it will surely resume its secret duties as America's main underwater spy. But the special sub probably won't be listening in on your phone and internet conversations. Too dangerous against military rivals and unnecessary for domestic surveillance, submarine wiretaps seem to have fallen out of favor.

You're still being spied on — just not by a submarine. Exactly what Jimmy Carter is doing is hard to say.

"I'm sure," Cote laughed, "it's up to no good."