1-27-2009, TUESDAY AFTER LUNCH MONEY MEMO
Heartland Payment Systems.(HPY) "OOPs"
by the Financial Foghorn

"Ignorance more frequently begets confidence than does knowledge."
Charles Darwin, Descent of Man

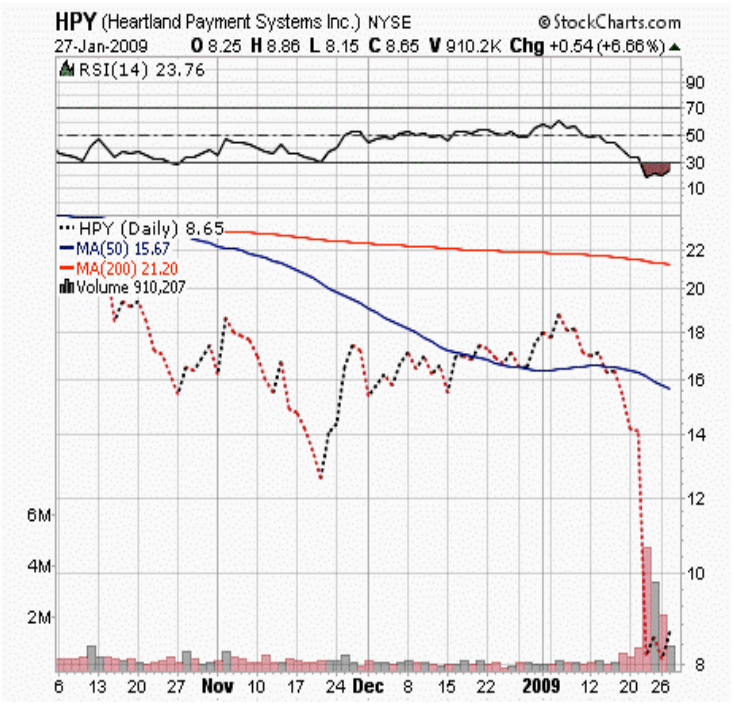
News Update: Ever heard of an outfit called Heartland Payment Systems? You may be hearing about them a lot.

Last Tuesday, January 20th, 2009, while the big shindig was going on in Washington D.C., Heartland, a large and heretofore unheralded processor of credit card slips, announced they were the victim of a computer break in.

Let me repeat that, Heartland Payment Systems announced something - in the hopes of being ignored - on the day of one of the splashiest Presidential coronations in our country's history. The company said, "By the way, our thought-to-be totally-secure computer system got hacked.

More than 100 MILLION credit card, debit card, and pin numbers that Heartland processes in a month were sucked out of the customer zone of safety and privacy and went off to Bulgaria, or the Ukraine, or Baluchistan somewhere."

The company wasn't really sure how many credit card numbers were stolen, or how bad the problem could be...so they tried to downplay the biggest private credit data theft in the history of the world as much as possible. Their announcement seemed to be saying, "Please enjoy the political show going on in Washington D.C. along with all the parties."



Heartland, which had annual revenues of $1.5 billion, and earned a little over $1.03 a share last year, is "concerned" about this hacker intrusion. I would guess they've made pretty good money over the years using high school students, homeless people, and barnyard animals to "process" over 100 million transactions a month for over 175,000 merchants, bars and restaurants. That merchant

user number probably won't be going up anytime soon. And it appears sellers have realized the seriousness of the problems as well, knocking HPY down from $14 on January 20th to $8 something today.

Heartland said in a *USA TODAY* interview that thieves and brigands gained access to Heartland's system with some sort of sneaky virus, for "longer than weeks" in late 2008. [The intrusion appears to be, or related to, the stame.exe virus that has plagued NASA and other government agencies.]

Heartland intimated that "discussions with the Secret Service and the Department of Justice give us a pretty good indication that this attack is part of a group of attacks involving crookedness." "Previously, hinted the spokesperson, "teenagers would break into computers just to brag to their girlfriends. Modern data thieves are driven by something called "greed," and are using stolen data to steal actual money from people. And they want to do it secretly. They may even have tried to steal money from other financial institutions." [Reports indicate there are some 20,000 to 25,000 "phishing attacks" occurring every MONTH now.]

Once it sorts out the matter, Heartland plans to notify each victim whose data were stolen, in order to comply with data-loss disclosure laws in more than 30 states. The company was heard to mutter, "If it weren't for those damn state statutes, we wouldn't tell anybody how fuckin' lame we were."

BUT WHAT ABOUT ME?

For customers, the problems are just beginning. The thieves could charge expensive goods on the card numbers now, or they could wait a few months until "the heat is off" and then begin using the cards.

Or, the criminal masterminds could just charge a small amount listed as a service charge of 50-99 cents on each of 100 million cards and figure that most of the card holders won't notice, and let the fee go through. (For those doing the math at home, a minimum of 50 cents each on 100 million cards equals $50 million dollars.)

HPY's invasion underscores the need for consumers to read EVERY line on their credit card bill and if it wasn't their purchase, call the teaser phone number on the back of your card. After scrambling through the phone tree and perhaps reaching a human being in India somewhere, the consumer

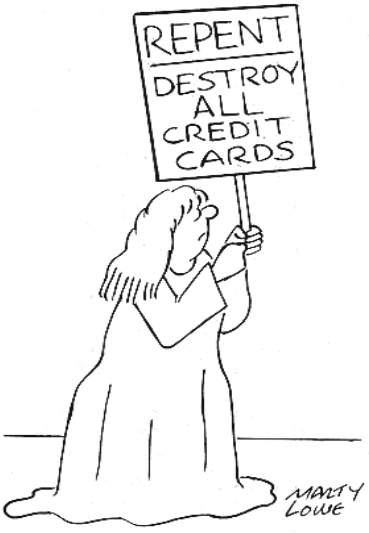
should yell "FRAUD" and high five their dog...or other appropriate house pet.

Once you whisper the magic fraud word, there are rules protecting customers in this area of EFTs (electronic fund transfers), known affectionately as FED Reg. "E." Assuming you have way too much time on your hands and feel like browsing some light FED speak, try: http://www.federalreserve.gov/bankinforeg/regecg.htm.

Reg E implies that you have 60 days from the date of your statement to complain, but if you have given notice in a timely manner, a credit card issuer must remove the item, and the company has the burden of proof to show that it's NOT fraud. And the credit card company must remove the item from your bill while the search for proof goes on.

If the card issuing bank can indeed show that you indeed bought 40 tires while visiting in Albania, then the burden, and the bill, shift back to you

If you don't believe in the current risk prevention measures of your card issuer, or you tend to think that the Ukrainians, et. al. might be ahead of the local plastic processors, ask for a new card and pin...NOW. Just say you believe your card has been compromised and that you want a new one. Usually that will be done, and while it's a minor hassle for both sides, it's certainly cheaper than having to pay for all those tires sometime.



Herewith a few prevention concepts:
1. Hey, don't use your card a whole lot. There seems to be a trend that carrying cash is "uncool" or something. And some persons think a debit card will always get them a cheeseburger, or whatever. (The Visa and Mastercard TV commercials disparaging the use of cash are doing a good job on this point.)

Well, Muffy, if the electric power goes out in a city - something that seems to be happening more frequently here in utility plant challenged America - you won't be able to buy gas, use an ATM, or get out of your parking garage without exact change money. Using your cards less will make it less likely that you'll get caught up in one of these increasingly frequent data thefts by Bulgarian keystroke grabbers. Carry some damn cash around.

2. When you use your card, don't let it out of your sight. In retail, this is usually pretty easy, a clerk will run it while you're standing at the register. In a restaurant, the wait staff tend to wander off to a back room card reader somewhere, and it's easy to swipe a card twice, and keep the second slip to use or sell later. Perhaps one should beware of wait persons who are wearing really good jewelry. There's a recent *Dilbert* cartoon where Dilbert gives his card to a wait staff, and she comes back wearing a mink coat. If Scott Adams can cartoon about it, it's really happening.

3. And if you use your card to buy something online, make sure the https// symbol is up in the URL line when you type a number in, and you're using secure encryption technology.

Given how likely it is that computers and credit card numbers can be hacked, the future looks like increasingly heavy security for card users, perhaps pictures on all cards, and more scrutiny on how we use our cards over the phone and on the web.

People who've bought precious metals in the past shouldn't have much trouble with brave new credit rules. Gold is a bearer instrument, owned by whoever possesses it. People who've handled gold don't take much for granted in dealing with the intangible financial world.

We should all remember the sergeant on *Hill Street Blues* who said, "Be careful out there."

Michael McGowan,
The Financial Foghorn, and author of
"Financial Foghorn's Guide to Gold--Get Rich, Get Happy, and Get to Heaven¨ with Monetary Metals."
www.FinancialFoghorn.com