



General Business Edition – June 2023

Even If You Weren't Part of the Harvard Pilgrim Health Breach (We were!) Here's what you need to do - NOW!

Although the Harvard Pilgrim Healthcare breach was several months ago, it only started being reported in May.

It's a severe breach because, according to Healthcare IT News, *"The stolen data includes names, physical addresses, phone numbers, dates of birth, health insurance account information, Social Security numbers, provider taxpayer identification numbers and clinical information"*

This statement is from **Harvard Pilgrim Health's** website: *"We take the privacy and security of the data entrusted to us seriously. Unfortunately, the investigation identified signs that data was copied and taken from our Harvard Pilgrim Health Care ("Harvard Pilgrim") systems between March 28, 2023, and April 17, 2023.*

We determined that the files at issue may contain personal information and/or protected health information for current and former subscribers and dependents, and current contracted providers. Harvard Pilgrim has now begun the process of notifying individuals whose information may potentially have been involved in the incident.

Additionally, while we are not aware of any misuse of personal information and protected health information as a result of the incident, out of an abundance of caution, Harvard Pilgrim is offering complimentary access to two (2) years of credit monitoring and identity



theft protection services through IDX to potentially impacted individuals. We also recommend that individuals remain vigilant, monitor, and review their financial and account statements and explanations of benefits, and report any unusual activity to the institution that issued the record and to law enforcement."

They are most likely mailing the information, so we don't know what you have to do to get the free monitoring and identity theft protection. ACTSmart is part of Harvard Pilgrim Health's network, so we will be getting letters as well. As of this writing, we have not received any notifications.

Here's what you need to do:

- **Change your password(s)**, especially if you have used your HPH password on other sites.
- **FREEZE** your accounts at the three major credit bureaus. This will keep anyone (even yourself) from opening a new line of credit. Don't worry; you can unfreeze your credit or temporarily lift a freeze for a set amount of time when you are ready to apply for a new credit card, line of credit, and allow access to lenders.

Experian - <https://www.experian.com/freeze/center.html>

TransUnion - <https://www.transunion.com/credit-freeze>

Continued on page 3

From The Desk of David Snell

In late May, we learned that our healthcare insurance company, Harvard Pilgrim Health Care was breached with a ransomware attack when it was reported on the news. As of this writing, we have had no official notice of the occurrence and only know what was stated on their website.

We don't know if they paid the ransom or how it happened. Did someone click on a malicious link? Was someone's password compromised? Were they breached through a back door in programming? We may never know.

What we do know is that if the bad actors got the information, as stated by Andrea Fox in *Healthcare IT News*, "***The stolen data includes names, physical addresses, phone numbers, dates of birth, health insurance account information, Social Security numbers, provider taxpayer identification numbers and clinical information,***" that we are in serious jeopardy!



The hackers have everything necessary to steal one's identity!

As you read our front-page article, you will see our STRONG recommendations to help protect you and your family. We have implemented these instructions ourselves, including a freeze on the minor children's credit accounts. Because they don't actually have credit accounts, Beth had to fill out forms for all three credit bureaus and mail them in along with their birth certificates, social security numbers, and other identifying information. She also sent them with the receipt requested because this is very sensitive information.

Pam and I have kept our credit frozen for several years because of another breach. It's a free service and keeps us safe.

I did have an incident where it caused me some embarrassment. A year ago, I was at a store that asked me if I wanted to open a credit card to save money on my purchase. When I responded "yes", my credit was denied! I was flabbergasted and confused! When I got home, I called the credit card company to give them a piece of my mind for putting me in that situation! They calmly told me that I had put a freeze on my credit and that they were just following my wishes!

If you'd like us to keep you in the loop as we maneuver through this situation, send an email to Pam@ACTSmartIT.com with the subject line of Harvard Pilgrim, and we'll let you know what we are doing to stay as safe and secure as possible.

Even if you weren't part of *this* breach, there's a good chance you'll need this info in the future!

Stay Safe!

BREACHED? Here's what you need to do - NOW!

Continued from Front Page

Equifax - <https://www.equifax.com/personal/credit-report-services/credit-freeze/>

- **Activate credit alerts** as soon as you get the HPHC information that gives you 2 years of FREE credit monitoring.
- **If your identity has been compromised** or misused, file an Identity Theft Report with your local police department.
- **Cybercriminals often sit on their spoils** for months until the turmoil dies down and our vigilance diminishes. Then, they'll use their ill-gotten gains with fewer chances of immediate disclosure.
- **Your healthcare insurance is also valuable** and can be sold on the Dark Web so, stay vigilant..

Experian offered valuable information and advice:

"Medical data is a big target for fraudsters because it's often much more valuable than other commonly available personal data. While a stolen credit card number might be sold for just a few cents, medical files can be worth as much as \$1,000 each, according to Mariya Yao, Chief Technology Officer and Head of Research & Design at TOPBOTS, an artificial intelligence research firm."

Signs that You're the Victim of Medical Identity Theft

Your first clue that your medical data may have been hacked might come in a statement, bill or notice from your insurer, your doctor or another medical provider, warns the Federal Trade Commission.

According to the commission you should be on the lookout for:

- A bill or statement of benefits showing medical services you didn't receive
- A call from a debt collector about a medical debt you don't owe
- One or more medical collection notices on

your credit report that you don't recognize

- A notice from your health plan or insurer saying you reached your benefit limit
- A denial of insurance because your medical records show a condition you don't have
- You also should keep an eye out for any unauthorized withdrawals or changes to your medical, insurance or financial accounts, notices of changes to your accounts, declined credit card charges, bounced checks and unexpected emails, notices or other inquiries about your accounts.
- In addition, notices of password changes or being locked out of your accounts can be signs that someone has logged on in your place.
- Finally, don't simply toss away a bill you don't recognize for a procedure you didn't have or from an unfamiliar doctor or medical provider, even if it's for someone under another name. Rather than being a mistake, it could be a sign that medical treatment is being obtained on your account by someone who's gotten a hold of your private information.
- Parents also should keep an eye out for any statements or activities relating to children or other family members who are carried on your insurance or who share the same medical providers.**

For more information:

<https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/>

*Minor children on your Harvard Pilgrim Health Insurance plan are also at risk. We suggest putting a credit freeze on their accounts at all three national credit bureaus. Since they have no credit on file, a form must be completed and mailed. Although it's more of a hassle than completing your requests on line, it protection that you don't want to exclude.

Don't Let An Expired Credit Card Bring

Picture this: you're just starting your day, sipping a sweet cup of coffee, and then you receive an unexpected call. Unfortunately, a business website is down!

Let us tell you; it's not a pretty scene! But it is one that one of our clients recently experienced. Their website, an essential tool for lead generation, was offline, and they were losing potential customers by the minute.

We didn't waste any time. Our website support team quickly acted to diagnose the issue and got the website back online as soon as possible. After conducting a thorough investigation, we discovered that the root cause of the problem was the credit card on file had expired earlier in the year.

Understanding the situation's urgency, we immediately contacted the client to inform them of the issue and take swift action. We updated the credit card information and expedited the renewal process for the domain to get it up and running as quickly as possible. Within an hour, the website was back online, and our client could breathe a sigh of relief and return to doing business online.

The Expired Credit Card Crisis

The consequences of prolonged website and email downtime can be catastrophic for a company, leading to a loss of credibility, customer trust, and financial stability. Without a website or email access, visitors can become frustrated, lose confidence in the brand, and ultimately turn to competitors. In addition, downtime can disrupt critical business operations, leading to missed opportunities, lost revenue, and decreased productivity.



Unexpected or preventable downtime can damage e-commerce businesses that use their website to generate revenue, maintain customer relationships, and provide an excellent user experience.

What Can Cause A Credit Card To Expire?

Credit cards can expire for various reasons, each with the potential to disrupt your online services if not appropriately managed. Let's discuss:

Issue Date - The most common reason for expiration is the card issue date. Banks and financial institutions typically set a fixed lifespan for their cards, usually between three to five years. After this date, new charges get declined upon activating a replacement card.

Original Card Reported Lost Or Stolen - Another reason could be the card on file was lost or stolen between renewal dates. Stolen or lost cards get deactivated immediately. Any pending charges get "declined," and a new card with a different number gets issued. However, this card number doesn't automatically update with vendors with the payment method on file.

Virtual Card Numbers - Virtual card numbers, or virtual account numbers, are valuable in combating fraud and increasing security in online transactions. Unlike traditional debit or credit cards, virtual cards

Your Business Website To A Halt!

are unique, one-time-use numbers generated for a specific purchase. With a variable expiration date that can get set based on a time or number of uses, this number could go invalid.

Changes In Bank Policies - As a bank's policies and offerings change over time, your current card may get phased out or expire. Other factors, including bank mergers, the financial institution shifting focus to different types of products or services, and responding to changes in regulations or market conditions, could affect account availability. In most cases, your bank will provide advance notice of these changes and provide options for switching to a different card or account.

Pro Tip: *It's crucial to stay aware of these factors and maintain up-to-date payment information with your website registrar.*

What Happens If My Domain Name Registration Expires?

Although domain renewal procedures and fees after expiration might differ among domain registrars, it is common practice for registrars to implement a "Grace Period" for a brief duration. This period typically spans 14-30 days, during which the domain owner can renew their domain without incurring additional costs or penalties.

This window provides a safety net for domain owners to act promptly and avoid losing their domain name to another interested party or having the registrar revert ownership and offer it for resale or auction.

In many cases, for a much higher price than the standard renewal fee. However, if the domain owner fails to renew within the Grace Period, the domain may enter a "Redemption Period." This stage, lasting around 30 days, often involves a considerably higher restoration fee than the regular renewal charge.

While redemption fees can vary, it is common for this fee to be \$150 or upwards. This one-time fee from the domain registrar covers restoring the domain to your account. The redemption fee only applies if the domain expires and is unrenewed within

the grace period.

If you cannot pay the redemption fee, you may still have the option to backorder the domain name. Backordering is a process where you request to purchase an expired domain name. If the domain name becomes available, all interested parties have a chance to acquire it through auction or direct sale. The biggest issue with this approach is it will cost significantly more than had you just renewed the domain in the first place.

Knowing this, it makes sense - and dollars - for business owners to stay vigilant and ensure that their business domain registration and payment information is up-to-date so they do not risk losing their valuable digital assets.

Avert Domain Renewal Disasters By Having A Website Support Team On Your Side

Partnering with a trusted website support team, like **Interactive Palette**, effectively prevents domain renewal or other website mishaps that can adversely affect your online presence. By entrusting your domain support and management to experienced professionals, you focus on core business operations while we handle the intricate details of domain registration, renewal, and maintenance.

Our experienced team ensures that your domain registration and payment information remain current, and we proactively monitor your domain's status to avoid any unexpected disruptions. With our reliable support, you can enjoy peace of mind, knowing that your valuable digital asset is protected and maintained by experts prioritizing your business's success.



Interactive Palette

**Mailing: P.O. Box 1007,
Fall River, MA 02722**

**Physical: 25 Braintree Hill Park
Braintree, MA 02184**

interactivepalette.com

(781) 930-3199

sales@interactivepalette.com

Three Tips for Effective Emails

There are many ways we communicate today, both in person and remotely, but often we stumble in our attempts.

1. **Email is a useful tool**, allowing us to keep a record of conversations, but we often miss the simplest way to grab a reader's attention and make it easy to find one amongst all the others: The subject line!

I recently looked through dozens of emails from a client, an author writing his first book, that he sent me in groups of chapters.

For the life of me, I couldn't find the last one that had chapters 7-10 in it.

Why?

Because the subject line was "For Your Review," as his earlier ones had been, too. My eyes just skipped right over it, until I backtracked slowly to find it.

What should have been included? Yes, of course: Chapters 7-10.

Sounds so simple, and it is. But we often overlook the impact our subject line can have.

2. **The physical setup** is often a barrier to great written communication, meaning we don't always realize what a huge block of text does to a reader. Too many writers use paragraphs that are both too long and not split with a full white space between them.

The best number of lines in any paragraph is about 9; more than that makes many readers dizzy. It's too easy to get lost in the middle of a paragraph that's 20+ lines long!

Now you may remember an English teacher telling you years ago that you couldn't create a new paragraph if you didn't have a new thought.

That was then. This is now.

The best advice I've ever gotten and always give

is to find a sensible enough spot in a huge paragraph and just start a new one. Your readers will thank you!

3. **The call to action**, something we don't always do. We just stop writing, which may leave the reader in the dark, wondering about next steps.

Something simple like "Check back with me tomorrow before noon" or "Let me know your thoughts" or even "This is for your files" at least gives a reader something to go by. Being specific cuts through the clutter and likely gives you both a satisfactory result.

All in all, email is a very useful and effective way to communicate, especially when we consider the impact to our readers.

I welcome your thoughts and ideas on this or any other communication method.



Susan Rooks

Grammar Goddess
508 272-5120

SusanR@GrammarGoddess.com

Monthly Supervisor Assessment of Employee Stability Report

This is #3 of Top Four Recommended Retention Programs to Launch in 2023.

This is a method for the senior leadership team to keep a pulse on the stability, or volatility of the workforce, before you are handed a resignation. The reason this is a monthly assessment is that the shift in employee sentiment can happen quickly. Often, information about employee issues surface when it is too late to repair or alter the outcome, and in many cases, the outcome is turnover. The supervisors in your organization make a determination each month regarding the stability of their workforce. It works like this:

Supervisors must turn in a report to their senior leader on each employee under their supervision, rating whether the employee:

- Will be here 1 = years from now (green)
- Will be here 6 – 12 months from now (yellow)
- Will be here 0 – 6 months from now (red)

Supervisors must also rate their employees individually as:

- Fully engaged
- Partially engaged
- Not engaged
- Actively disengaged

The Senior Leader then communicates with HR and the CEO regarding the trends of the assessment. This is a good way for Senior Leaders to hold their supervisors accountable for employee

retention as well, as patterns do tend to show up in these monthly reports.

Outstanding leaders tend to shine on these reports. When a manager completes the report showing positive engagement, yet the results are contradictory, i.e. losses, performance issues, and other negative events, the Senior Leader knows that the leaders needs help.

For those employees who are at risk of leaving the organization, barring performance issues and a formal exit strategy to move the employee out of the organization, (which HR should have been a part of developing), HR and senior management will collaborate to develop a **Retention and Engagement Plan for each employee at risk, to avoid the potential loss.**



This program should help you avoid being blindsided by resignations.



Debra J. Parent, PHR, SHRM-CP, CHHR

rightfitrecruiting@comcast.net

(508) 884-6798

<https://rightfitrecruiting.com/>

Or connect with Deb via LinkedIn –

<https://www.linkedin.com/company/djp-right-fit-recruiting-llc/about/>

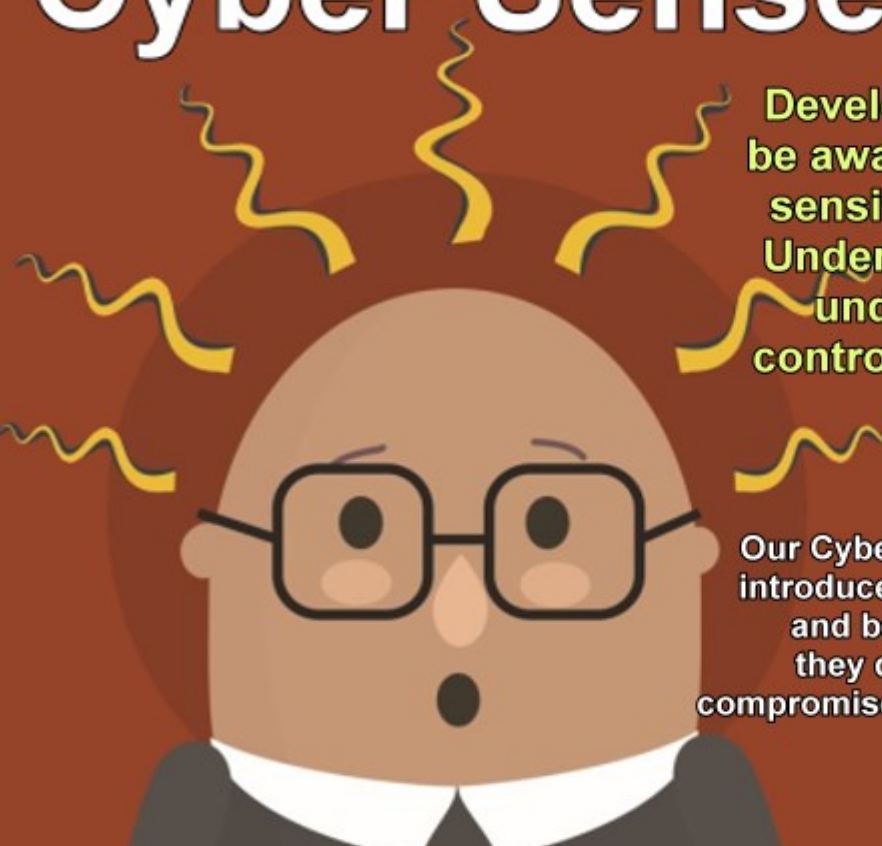
You can view Debra's recent webinars at:

<https://actsmartit.com/recruit>

In This Issue:

- Are you part of the Harvard Pilgrim Health breach? (We were!) Here's what you need to do - NOW!
- Don't Let An Expired Credit Card Bring Your Business Website To A Halt!
- 3 Tips for Effective Emails
- Monthly Supervisor Assessment of Employee Stability Report
- And MORE!

Cyber Sense



Develop your cyber sense and be aware of how to protect your sensitive information online. Understand online threats and understand that you have control to defend against them.

Our Cybersecurity Training is designed to introduce every employee to the "basics" and best practices in cybersecurity, so they don't have "one wrong click" that compromises the entire company's network. Easy and Affordable!

ActSmartIT.com/training