ACT SMART I.T.
www.ACTSmartIT.com
General Business Edition — September 2024

Hackers Probably Have Your Social Security Number from a Massive Breach

Last year, we reported that we were part of the Harvard Pilgrim Health breach. At that time, we provided instructions on how to maneuver these challenges.

With the announcement of another possible breach affecting billions of individuals, we are reissuing and updating this information to help you stay safe.

This new National Public Data breach is monumental, and it's safe to assume you're at risk. The hackers put the entire database — which includes Social Security numbers, full names and addresses on the Dark Web for sale, and when it didn't sell for the $3.5m that they wanted, they handed it out for free!

Below is a verified website where you can check if your data was included in the breach. The compromised data appears to be from an older backup, as it may not contain your current address information.

https://npd.pentester.com/

Here's why it matters:

If your Social Security number is stolen and used for someone's gain, like opening up a loan or getting a job, start with the Federal Trade Commission's IdentityTheft.gov ***(https://www.identitytheft.gov/Steps***). Fill out the form there, and you'll get an entire plan for how to recover your identity and protect yourself going forward.

The IRS also has a place to report if you suspect someone is using your SSN: ***Identity Theft Central*** (**https://www.irs.gov/identity-theft-central)**. Major red flags to watch for? You receive a tax form for a job you didn't do or you submit your taxes and there's already something on file. You know things are bad when both the FTC and the IRS have dedicated portals to help you because someone is using your SSN and stealing from you.

ACT SMART I.T.
Helping You Benefit From Today's Technologies

Our recommendations:

- **Change your password(s), especially if you have used your passwords on other sites.**
- **FREEZE your accounts at the three major credit bureaus.** This will keep anyone (even you) 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 like when you are ready to apply for a credit card, and allow access to lenders.

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

TransUnion — https://www.transunion.com/credit-freeze

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

- **Activate credit alerts**

If your identity has been compromised or misused, file an Identity Theft Report with your local police department.

Continued on page 3

From The Desk of David Snell

Welcome September!
Though we're getting ready to hunker down for the final stretch of the year, the weather seems to have other plans! With such beautiful days gracing us, it feels like summer is begging to stick around just a little longer.

As I write this, we're surprisingly in the clear this hurricane season—so far, at least. Let's hope I didn't just jinx it! Despite the quiet skies, it's always a good idea to be prepared.

Pam has put together a helpful infographic, *"Safeguard Critical Documents and Valuables,"* which you can easily request on our website: https://actsmartit.com/safeguard-documents-valuables/ It's a useful resource straight from FEMA, and it's valuable year-round, not just during storm season. While you're there, be sure to explore our **Infographics Archive** for other helpful tips Pam has curated.

Our front-page feature this month is the kind of thing that can keep anyone up at night: *"Hackers May Have Stolen Your Social Security Number in a Massive Breach."* Definitely check out the verified link provided to see if you've been impacted. Both Pam and I were involved in this breach, but we've had our credit frozen for years now. It's a good practice and helps me sleep a little easier, though staying vigilant is always key.

Speaking of staying alert, **Vinny Pircio** from Wareham Banker is back with another installment of *Scam Alert!* This month, he dives into the *Fake Bank Call Scam*, a reminder to always be cautious. Even if you're too savvy to fall for it, I recommend showing the article on page 7 to any friends or family members who might not be as careful—you never know who these scammers could target next!

Pam has also been hard at work updating our **OfficeManagersSociety.com** website, packing it with fresh content that we couldn't fit into these eight pages. If you're curious, hop over and take a peek!

On a lighter note, my garden has been nothing short of abundant, even with the lack of rain. We're drowning in cucumbers, and the scarlet runner beans are so tall, I've had to break out the ladder!

And finally, a little family update: Sarah just celebrated her 8th birthday on September 1! Can you believe how time flies? It feels like we were just sharing her baby pictures. We managed to sneak in one last summer adventure at Wicked Waves on the Cape, and the kids had an absolute blast at the water park.

What a way to end the season!

· **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. It's not unusual for companies to say that they are unaware of breached information being used at the time they disclose the breach.

· **Your healthcare insurance itself is also very valuable** and can be sold on the Dark Web, so stay vigilant.

Minor children may also be 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 online, it is protection that you don't want to exclude. For more information, read: **https://www.equifax.com/personal/education/identity-theft/child-identity-theft/**

THE CURRENT
TECH ALERTS
POWERED BY **KIM KOMANDO**

Kim Komando issued a special Tech Alert on August 15.

A fake tax form is one thing, but most signs of identity theft are more subtle — at least, in the beginning. Here's what to look for, along with steps to lock down your identity and protect your money:

· **Double-check all healthcare communications.** If you get an explanation of benefits (EOB) or bill for services you didn't receive, contact your health care provider and insurance company ASAP. It likely means someone is using your benefits for their own care.

· **Treat email requests with caution.** Be skeptical of anything that seems super urgent. It's OK to slow down for safety.

· **Freeze your credit.** *See our ACTSmart tips page 3*

· **Be wary of "old friends" who appear out of nowhere.** It could be a hacker who happens to have a little (stolen) info. Take the time to confirm they are who they say they are.

· **Make a list of exposed data.** Keep this digitally or on a Post-it. Be suspicious of anyone who references it in an email or phone call. Say the company you financed your car through was hacked. Alarm bells should sound if you get a call out of the blue about a major issue with your loan.

· **Update your PIN and banking login credentials,** even if they weren't involved directly in a breach. Keep an eye on your bank and credit card statements for anything out of the ordinary. Set up banking alerts on your phone while you're at it.

·**What to get Kim's Free daily newsletter?**
https://join.komando.com/ef9e99759

Would you like a print copy of this article mailed to you?

ACTSmartIT.com/stolen-ss-number to request this FREE Infographic

Benefits of Blogging on Your

Savvy business owners and organizational leaders always seek innovative ways to connect with customers, build relationships, and establish trust with the public. Among the most powerful tools they can leverage today is a blog.

Adding a blog to your business or organizational website can transform your online presence and offer many benefits. Blog entries can engage your audience in new and exciting ways. Let's explore how adding a blog can benefit your business.

Establish Your Brand Personality

A blog serves as a canvas to paint your brand's personality. It's where you share your values, stories, and expertise.

Are you a fun, quirky company, or are you more serious and professional? Your blog helps communicate more about who you are, your values, and what you represent.

Regular posts and updates offer the opportunity to showcase new products, share industry or company news, and strengthen your connection with friends, fans, and website visitors.

Boost Your SEO

Search engine crawlers live to discover fresh, relevant content. Adding a business blog to your website and making regular updates increases your chances of ranking higher in search engine results.

Each new blog post is an opportunity to include links back to other core pages of your website, such as product pages or email opt-in forms.

It also gives you something new and fresh to share on your social media profiles, potentially driving higher visibility, traffic, and potential customers to your business or cause.

Engage Your Audience

Blogs are a sensible approach to engaging with your audience. It's a holistic platform to share updates about your products, services, and company news. Are you planning an event? Is there a new product launch in the works? Is your company offering a special promotion? Announce these things on your blog. Updated information keeps your audience informed and excited about what's happening in your business.

Showcase Expertise and Authority

Sharing expertise, knowledge, and tips through blog posts helps establish industry authority. Whether you're giving advice, creating how-to guides, or sharing industry insights, your blog becomes a valuable resource for your readers. This expertise positions your business as a go-to source for information, increasing your credibility and trustworthiness.

Business Website

Drive Traffic to Your Website

Every blog post you publish gives you another opportunity to appear in search engine results, ideally for targeted keyword phrases that can convert into sales opportunities.

Nurture Customer Relationships

Blogs allow direct, more-personal engagement with potential customers. Encouraging comments and feedback on your posts opens up a dialogue with your audience. Interacting with visitors empowers you to understand their needs and preferences better. It also shows your customers that you value their opinions and are willing to engage with them, strengthening your relationship.

Highlight Customer Stories and Testimonials

Word-of-mouth remains very powerful in marketing. Consider using your blog to highlight customer feedback and testimonials. Share successful stories of how your products or services helped solve problems or improved lives. These stories build trust and inspire potential customers to choose your business over competitors.

Create a Hub for Other Online Activities

Your blog is an ideal central hub for all your online activities. Link your social media posts back to your blog, integrate it with your email newsletters, and use it as a platform to drive your overall digital marketing strategy. This comprehensive approach ensures that all your online efforts are interconnected and working together to enhance your brand's visibility and impact.

Support Community and Give Back

A blog is a great platform to support your community. Share stories about local events, highlight partnerships with other businesses, and showcase your involvement in charitable activities. Giving back helps create a greater sense of community and portrays your company as one that cares and contributes positively to society.

Increase Conversion Rates

Well-crafted blog posts can also help increase your conversion rates. When you provide valuable information and address your audience's pain points, you guide them through their buying journey. Include clear calls to action (CTAs) in your posts to direct readers toward the next step:

- **Signing up for a newsletter**
- **Making a purchase**
- **Contacting you for more information**

Being able to direct visitors to conversion pages boosts direct revenue. You can also provide a contact phone, chat, or phone number to speak with people who need more information.

FAQs?

https://www.interactivepalette.com/benefits-of-blogging-on-your-business-website/

Kevin McNally, Interactive Palette

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

Physical: 25 Braintree Hill Park, Braintree, MA 02184

interactivepalette.com sales@interactivepalette.com

(781) 930-3199

UPDATING YOUR POLICIES - The "CROWN ACT"

The acronym CROWN, within the CROWN Act, refers to "Creating a Respectful and Open World for Natural Hair." Such legislation prohibits discrimination based upon hairstyle that is commonly associated with a race or national origin.

While there isn't a federal prohibition at this time, currently around 2 dozen states have enacted this law, including Connecticut, Maine, Massachusetts, New York, and New Jersey.

New Hampshire recently enacted the CROWN Act, which takes effect in that state on September 1, 2024.

Two areas where your employee handbook must be updated:

- Employers should be taking a second look at their dress and grooming policies to ensure that such policies do not violate the protections of the CROWN Act.
- This legislation should be referenced within your anti-discrimination policy.

What if certain hairstyles cause a safety problem for your particular business in terms of your legitimate business needs? As always, open communication, with a discussion as to ways to address and adapt to those concerns, must take place.

Attorney Helene Horn Figman combines specialized legal knowledge in employment law with the skills and perspectives uniquely suited to Human Resources Consulting. www.figmanlaw.com

Information about her anti-harassment and anti-discrimination education programs can be found at www.workplaceawarenesstraining.com

This article has been prepared by the Law Offices of Helene Horn Figman, P.C. for general informational purposes only. It does not constitute legal advice and is presented without any representation of warranty whatsoever.

Helene Horn Figman

Law Offices of Helene Horn Figman, P.C.

Employment Law & HR Resource Management

45 Bristol Drive Suite 207, South Easton, MA 02375

FigmanLaw.com hfigman@figmanlaw.com

508-238-2700

Scam Alert!

With so much of our lives being digital and with more and more of our banking being done electronically, it is more important than EVER to make sure you don't become a victim of fraud.

This month, we're talking about a scam that has been very common in the last few months and has affected many people and banking institutions. This scam is the ***Fake Bank Call Scam.***

This scam is one of the more infamous scams that I have seen in the last few months and in my opinion, the most successful for the scammers. This scam starts with a phone call from your banking institution; surprisingly, they can spoof your bank's phone number. For example, you may get a call that will show on your caller ID as the bank's phone number. Any average person would assume that their bank is calling them for a valid purpose, which is how they start earning your trust.

Once they have you on the phone, they will indicate that they are calling from "your financial institution" and ask if you authorized a transaction in a location you have not been to. For some reason, they tend to tell customers that the fraud occurred in New York City. If you hear this, it should raise an immediate red flag. Now, most people would be frustrated, anxious, or even scared. This is part of their plan to get them to trust you.

Next, they will ask you to confirm your debit card number, PIN, and Balance. **Banks will never ever ask for your PIN (or online banking password).** If anyone from a "financial institution" ever asks for a PIN, it's another red flag. Once they have your card number and PIN, they can make a fake card and start charging purchases to your account. As soon as they have this info, it will be too late.

There are ways you can protect yourself from this scam.

- Be aware that this is happening. Many people trust their bank, and if they don't know this scam is happening, they are more likely to trust the individual on the phone.
- Listen closely for red flags; some examples are below:
  - Asking for your PIN
  - Asking for an online banking password
  - Saying you've "had fraud in New York City"
- Call a trusted bank representative
  - Reach out to your local banker.
  - If you do not have a local banker you are familiar with, hang up. MMEDIATELY and call your financial institution to confirm the call.

Fraudsters are everywhere and are getting sneakier by the day. It's more important than ever to make sure you are protected and your hard-earned money remains yours!

Vincent A Pircio, Branch Manager II,

Rockland Trust

2995 Cranberry Highway, East Wareham, MA 02538

Phone (508) 295-6900 | Fax (508) 295-7178

Vincent.Pircio@RocklandTrust.com

ACTSmart IT
332 Main Street
Wareham, MA 02571

In This Issue:

This newsletter was thoughtfully edited by Susan Rooks, the Grammar Goddess, so we can look and sound as smart as we are.

Susan Rooks
The Grammar Goddess
https://www.linkedin.com/in/susanrooks-the-grammar-goddess/

Tech Tip:

Zero Click Exploit

Zero-click exploits are cyber attacks that infect your device *without requiring any clicks*. They usually target messaging or voice-calling apps, using hidden messages or files to deploy malware.
Since these attacks don't leave much evidence, they're tough to spot.

To stay safe...

- **Make sure your software is always updated**
- **Make sure your team doesn't open messages or take calls from unknown senders.**

For FREE weekly tips, sign up at ACTSmartIT.com/tips