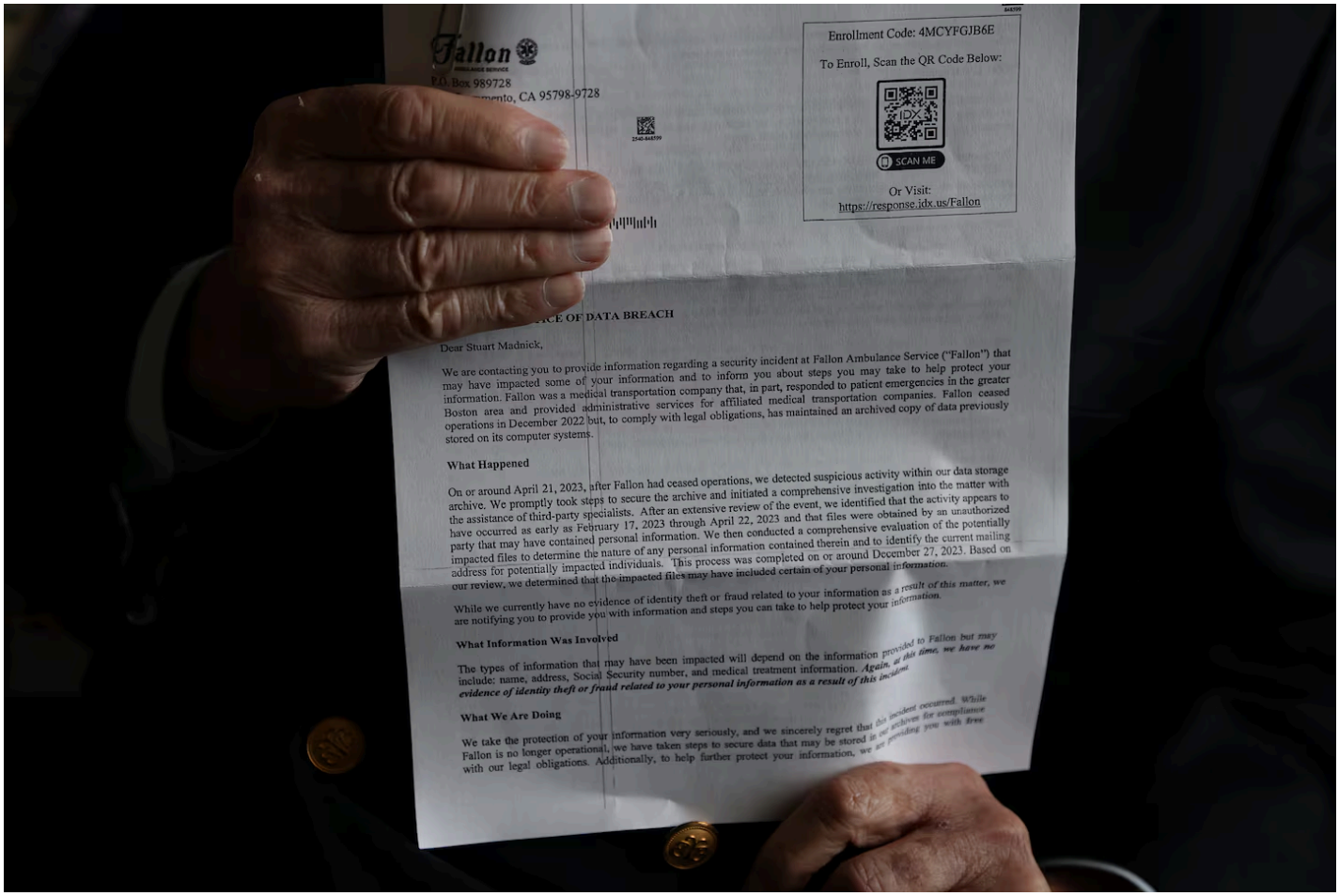
‘Don’t assume you are safe’: Data breaches soar, with nearly 7 million Mass. accounts hit in 2023

By **Scooty Nickerson** Globe Staff, Updated October 25, 2024, 6:07 a.m.



Stuart Madnick, professor at MIT, held one of the letters he received regarding data breaches. He is codirector of the MIT flagship cybersecurity consortium. SUZANNE KREITER/GLOBE STAFF

The Uber ride to Boston was already booked when Denise Micale, 69, of Westport noticed a $990 charge on her bank statement late last summer for a livestock feeding machine that she, a retired nurse, doesn’t remember buying.

Then she remembered an invoice she got in her email that she ignored. “Sometimes you get these emails from people and they’re bogus,” she said.

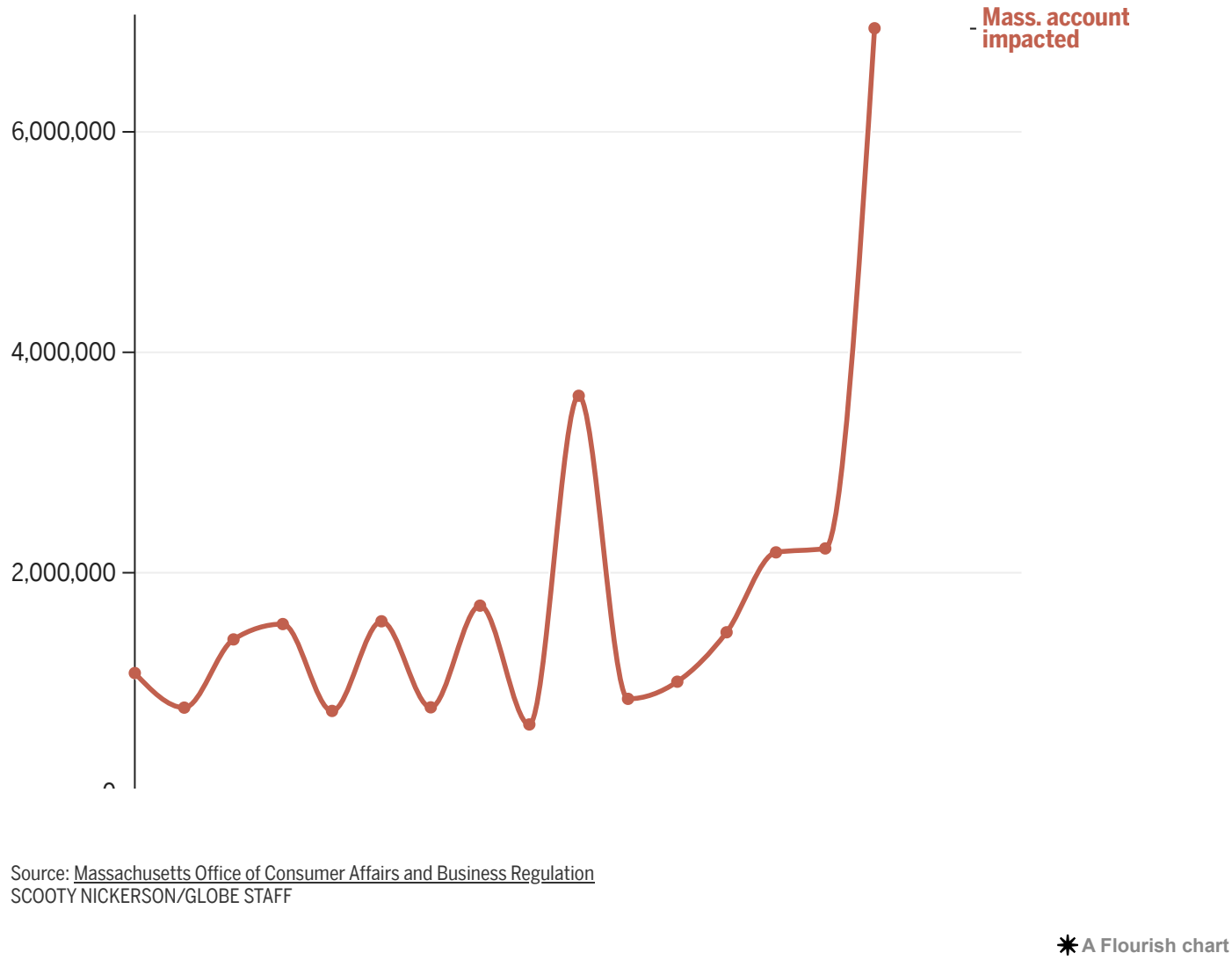
Micale remembered another email that summer: one from Southcoast Health, her health care provider, that her personal data had been part of a data breach of their systems.

Micale said she quickly called up her bank and put a freeze on her account. But that put her trip to Boston with her husband, the first after over a year of long COVID, on hold.

“It was really stressful,” she said. “I had to cancel all my reservations and start over from scratch.”

Micale is far from the only Massachusetts resident to be impacted by a data breach in recent years.

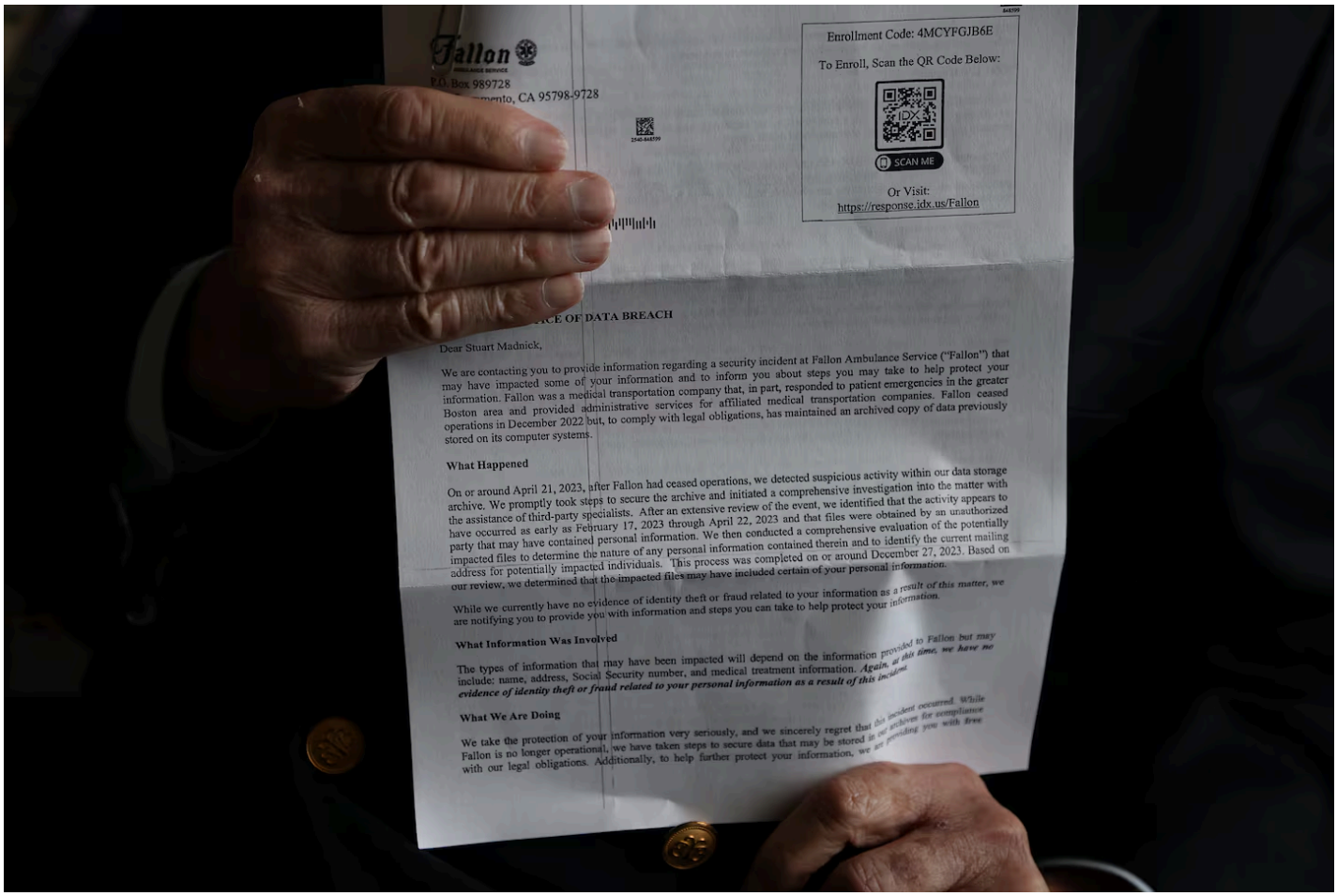
A new Globe analysis of state data shows just how off-the-charts the problem has become. In 2022, 1.9 million Massachusetts resident accounts were impacted by data breaches. The following year, that number spiked to more than 6.9 million accounts, fueled in part by large-scale breaches, including one that affected more than 2 million Harvard Pilgrim Health Care accounts.



So far this year, the numbers are already above the historical average, though not quite as striking as 2023, with 1.8 million accounts breached through September.

The overall uptick is “a trend around the world,” said Stuart Madnick codirector of MIT’s flagship cybersecurity consortium. “It’s no surprise that Massachusetts is part of the uptick.”

As more data than ever, including sensitive personal banking and health care information, is stored on the internet, breaches are becoming increasingly common, he and others said. Meanwhile, hacker groups are also becoming more sophisticated, putting more people at risk of fraud and identity theft.



Stuart Madnick, professor at MIT, held one of the letters he received regarding data breaches. SUZANNE KREITER/GLOBE STAFF

Across the United States, an estimated 353 million accounts fell victim to data breaches last year, according to the Identity Theft Resource Center, a national nonprofit that provides cost-free assistance to identity theft victims. The total number of breaches was 72 percent higher than the previous record year of 2021.

Data breach victims can suffer serious financial and personal repercussions after their information is compromised. For consumers, their financial information could be sold on the dark web, where scammers can purchase it and rack up debt in their name.

The burden of dealing with the consequences, such as contesting fraudulent charges, often falls on consumers.

Doing so can prove challenging even for tech-savvy people like Leigh Graham, a Johns Hopkins researcher, whose personal data has been breached at least twice in the past year, including when her employer was breached.

Graham, who lives in Northampton, said she struggled to navigate credit bureau websites to freeze her credit report after she noticed that someone spent $550 on Ticketmaster in her name.

“I feel like I don’t understand what I’m looking at,” she said. “The onus is so on the individual consumer to fix everything.”

Companies impacted by data breaches may find themselves paying hefty ransom to keep their clients’ data from being published online.

That’s what happened to Change Healthcare, a subsidiary of United Health, a national conglomerate. It paid a $22 million ransom earlier this year to a hacking group that stole protected health information from their systems. The health care group acknowledged that the stolen data could include information on a “substantial proportion of people in America.” Massachusetts data indicates that tens of thousands of residents were caught up in the breach.

Screenshots of some of the hacked data ended up online, despite the ransom payment. The hack also reportedly led to problems for patients in getting prescriptions approved at hundreds of medical facilities across the country.

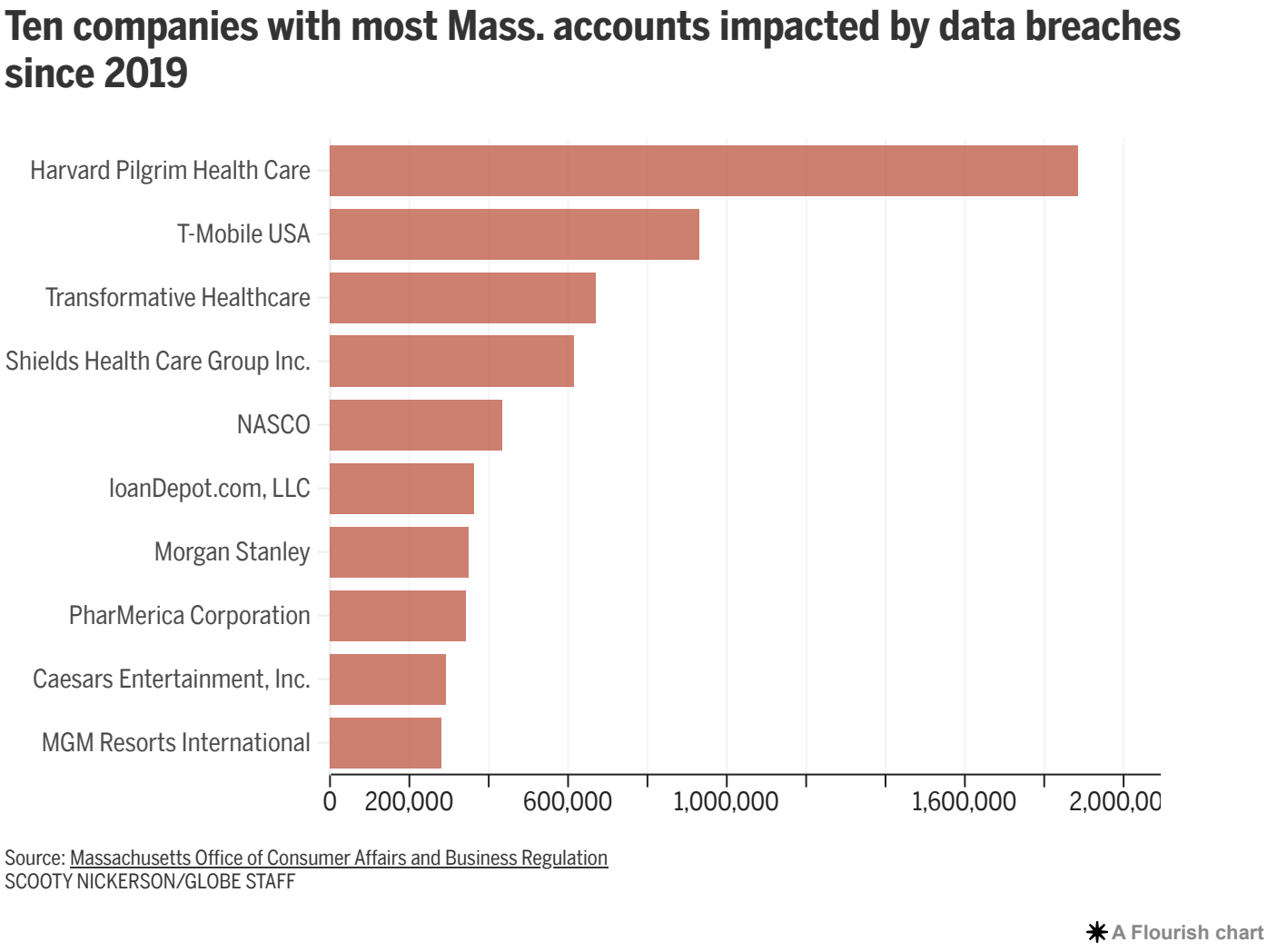
In Massachusetts, both national behemoths, like T-Mobile, and smaller organizations, like the Roman Catholic Diocese of Fall River, have been hit by data breaches in recent years, data shows. Even state government employees have been targeted.

At smaller organizations, experts say it’s a daunting task for IT teams with limited resources to compete with large international hacking organizations.

“A lot of [small] organizations have to face a cost-benefit tradeoff, and sometimes just have to accept a certain level of risk,” said Saroja Hanasoge, director of advisory services at CyberTrust Massachusetts, which partners with cities and organizations across the state to beef up their cybersecurity.

The largest reported hack affecting Massachusetts residents since 2017 happened last year, when Harvard Pilgrim Health Care revealed a breach that affected over 2.1 million state client accounts. Harvard Pilgrim is a subsidiary of Point32Health, the second biggest health insurance company in the state, and provides coverage at dozens of hospitals in Massachusetts alone.

In an open letter written to clients after the hack, the nonprofit said hackers may have gotten access to files containing client names, Social Security numbers, dates of birth, tax identification numbers, and patient clinical information, such as medical diagnoses and treatments.



“We want to assure you that we are taking this incident extremely seriously, and we deeply regret any inconvenience this incident may cause,” the group’s letter said.

A spokesperson for Harvard Pilgrim declined to speak about the breach.

Bad actors are becoming more sophisticated

Experts say it's now far easier for bad actors to go online and buy hacking services at low cost, often using cryptocurrencies like Bitcoin.

For-hire hacking groups do a lot of the technical work that everyday thieves would ordinarily not have the know-how to pull off, said Kevin Powers, director of the cybersecurity program at Boston College. Some of the hacking groups even offer affordable subscriptions.

For as little as $40 a month "you can get yourself a monthly subscription for a criminal enterprise," Powers said.

He added that schemers also now use artificial intelligence services available on the dark web that are built to make hacking easy. Many hacking groups have begun using the AI services to make highly personalized phishing emails that are much harder to spot as fraudulent.

Even in cases where federal investigators manage to shut down a big hacking network, they will often reappear online, sometimes from a different country.

Hackers also have the benefit of bigger and easier targets to crack in recent years, as a growing number of companies are putting troves of data on poorly set up cloud servers with minimal protections.

"The bad guys are getting badder faster than the good guys are getting better," Madnick of MIT said.

Some of those bad guys have even managed to break into Madnick's accounts multiple times.

"You can be the most careful person in the world and there is no way to guarantee they won't break in," he said. "Don't assume you are safe."

Scooty Nickerson can be reached at scooty.nickerson@globe.com.

Show 31 comments