Why Rewards for Loyal Spenders Are ‘a Honey Pot for Hackers’

The punch cards stuffed in your wallet know next to nothing about you, except maybe how many frozen yogurts you still need to buy to get a free one.

But loyalty programs, as they shift from paper and plastic to apps and websites, are increasingly tracking a currency that can be more valuable than how much you spend: personal data. As a result, the programs know things about you that some of your friends may not, like your favorite flavor (mango), when your cravings strike (early afternoon) and how you pay (with your Visa), in addition to billing details and contact information.

Hackers are in close pursuit.

One loyalty-fraud prevention group estimates, conservatively, that $1 billion a year is lost to crime related to the programs. As a share of fraud not involving a physical payment card, such schemes more than doubled from 2017 to 2018, according to the Javelin Strategy & Research firm.

Some criminals use stolen credentials to impersonate customers, breach loyalty profiles and then tap into separate accounts. Others deplete balances or sell points on dark web marketplaces. One hacked Southwest Airlines rewards account with at least 50,000 miles was advertised for $98.88, according to the cloud security company Armor.

In a data breach revealed last year as one of the largest ever, thieves attacked Marriott’s Starwood unit, stealing the personal information — including five million unencrypted passport numbers — of more than 350 million customers and Starwood Preferred Guest members. Data stored in Dunkin’ Donuts’ DD Perks program was also exposed in an attack disclosed last year.

This year, several McDonald’s customers in Canada complained that criminals had breached their accounts on the chain’s loyalty app, My McD’s, and placed unauthorized orders, some totaling more than $1,000. A McDonald’s spokesman said that the company was aware of “some isolated incidents” involving fraudulent purchases but was “confident in the security of the app.”

Loyalty programs are “almost a honey pot for hackers,” said Kevin Lee, a risk expert for the digital security firm Sift. They tend to be, he said, “the path of least resistance”: easy to sign up for, shielded by flimsy passwords and often neglected by users. The programs, and their appetite for data, have grown, but security has not kept pace.

Daniel Najera was hit twice.

On April 9, he received a series of emails about his Hilton Honors account. Within an hour, the account had been linked to Amazon and all 80,000 of his Hilton points had been used to make purchases.

He said he had not taken those steps, and he feared that his Hilton account information, including his credit card number, might have been stolen.

Hilton said it had “the appropriate security and fraud protection measures in place.” The company also said it had reinstated Mr. Najera’s points after he reported the intrusion.

Mr. Najera, a chef who lives in Saginaw, Mich., said something similar had happened to his Buffalo Wild Wings loyalty account earlier this year.