Data Breach Alert:

Inside the Hy-Vee Data Breach

What Happened

5.3 Million

According to Krebs On Security, the breach is tied to the sale of 5.3 million new accounts from cardholders in 35 states.

245 Stores

Credit card credentials from a point-of-sale data breach were impacted across Hy-Vee's restaurants, fuel pumps and drive-thru coffee shops

8 States

Hy-Vee operates in the Midwest in Illinois, Iowa, Kansas, Minnesota, Missouri, Nebraska, South Dakota and Wisconsin

What You Need to Know

- Hy-Vee said they discovered unauthorized activity on some of its payment processing systems.
- The store hired a cybersecurity firm, notified federal law enforcement and payment card networks.
- The investigation is focused on card transactions at its fuel pumps, coffee shops, and restaurants
- The company uses point-to-point encryption for processing card transactions to protect customers.
- Krebs' report cited two unnamed sources and said the data is being sold under the name "Solar Energy" in a data dump for between $17-$35 each.

"We are aware of reports from payment processors and the card networks of payment data being offered for sale and are working with the payment card networks so that they can identify the cards and work with issuing banks to initiate heightened monitoring on accounts."

- Hy-Vee spokesperson Tina Pothoff.

What To Do About It

- ❑ Educate cardholders about the incident and how to flag fraudulent charges.
- ❑ Review data to determine if their cardholders hopped at Hy-Vee.
- ❑ Track the fallout of the breach to identify potential Incidents from stolen card data.
- ❑ Inform cardholders about common fraud scams that occur with stolen credit card data.
- ❑ Monitor potential fraud In real-time to get ahead of incidents before they spread.
- ❑ Offer extra fraud/credit monitoring to proactively protect your customers.

Rippleshot

Stopping Fraud at the Speed of Data