# Baxter Strikes With Matchlight for Dark Web Monitoring, Fraud Detection

By Roy Urrico
August 21, 2017 •


There is growing fear the internet's deep recesses could hold detailed information that threaten credit unions organization and

members. Dark web monitoring and fraud detection could alleviate some of those concerns.

Fraud is on the rise. The Nilson Report indicated card fraud will grow from $21.84 billion in 2015 to $31.67 billion in 2020. FICO data also confirmed card-skimming losses climbed a massive 546% between 2014 and 2015, and another 70% between 2015 and 2016.

Then there is breach fallout. Individuals with payment card data exposed in a data breach are three times more likely to become victims of identity fraud, according to Javelin Strategy & Research. A recent IBM/Ponemon study revealed the global average cost of a data breach is $3.62 million; and the average cost for each lost or stolen record containing sensitive and confidential information is about $140.

For credit unions, the risks could be worse. "Credit unions face greater existential risks from fraud and information security incidents than do larger financial institutions." said Tyler Carbone, chief product officer of Baltimore-based dark web intelligence company Terbium Labs. That is because when an incident does occur, the potential damage represents a much greater percentage of their balance sheet.

Some credit unions are turning to next-generation information security solutions such as Terbium Labs' Matchlight comprehensive, dark web data

RELATED

**How to Protect Members From Dark Web Data Markets**

monitoring system to mitigate the hazards.

On the dark web, fraudsters shop the bargain bin for card data but are willing to pay more for complete...

Recently Terbium Labs announced that the $2.8 billion Vernon Hills, Ill.-based Baxter Credit Union – a full-service financial institution providing SEG and community banking to members in all 50 states and Puerto Rico – selected Matchlight for continuous dark web data monitoring, fraud detection, and information security-risk assessment.

“Fraud evolves constantly, and you can’t afford a ‘set it and forget it’ mindset with your information security solutions," Martin Hetzel, senior information security analyst at BCU, said. "To help protect the personal information of more than 200 thousand members, we needed a proactive solution, one with the scale, speed, and precision to quickly identify and rapidly counter information theft and fraud.”

Given the task to consider dark web threat intelligence in the February/March 2017 timeframe, Hetzel and Stacy Hogan, BCU fraud manager, explained their BCU cybersecurity and fraud teams evaluated, researched and investigated services. The credit union decided Matchlight was the best fit for the organization because of the platform’s ease of use and data presentation. In addition, Terbium provided a dedicated analyst on the Terbium side.

“From a fraud perspective, we were excited to look into the space as we have a large network of other credit unions that we deal with from the fraud aspect,” Hogan pointed out.

Carbone noted BCU was looking for a solution that would provide them with visibility in two keys areas: information security and fraud use cases.

*Read the full article in the Aug. 30 edition of CUTimes.*