Patelco Credit Union Settles Class Action Cyberhack Suit for $7.25M

The company's data breach keeps some 'scared' victims on guard.

Mia Nagano/San Francisco Public Press

Patelco Credit Union, which has settled a class action with customers whose personal information was stolen in a massive data breach last year, operates 36 branches in and around Sacramento and the greater Bay Area, including this one in Berkeley.

06.09.2025 | by YURI NAGANO

Nearly a year after a ransomware attack paralyzed Patelco Credit Union, a class action against the nonprofit financial cooperative has been settled for $7.25 million. More than 1 million accounts were affected by the breach.

Dublin-based Patelco has reached a settlement with 12 named plaintiffs in Alameda County Superior Court, said Scott Edward Cole (https://colevannote.com/scott-edward-cole-attorney-founder-profile/) , an Oakland consumer lawyer for Cole & Van Note representing the account holders.

Cole said the plaintiffs are waiting for the court to formally approve the settlement (https://www.documentcloud.org/documents/25967020-24cv082095/) so the documents can be sent to other members of the class after a hearing scheduled for June 10.

Settlement terms include creating a $7.25 million fund to be shared by victims affected by the ransomware attack and system shutdown of Patelco that lasted for more than two weeks last summer.

Patelco has acknowledged that hackers gained access to account holders' names, dates of birth, home addresses, Social Security numbers, driver's license numbers and email addresses. The credit union has offered complimentary credit-monitoring subscription services to all data breach victims.

Plaintiffs in this case "have various ways of demonstrating that the damages they suffered were traceable to the Patelco data breach," Cole said. Plaintiffs sued Patelco for negligence and violation of the California Consumer Privacy Act, and "negotiations were adversarial" in nature, according to the settlement.

Meanwhile, the San Francisco Public Press found leaked data from the cyberattack posted on the dark web — part of the internet that can be accessed anonymously and is not indexed by search engines — and reached out to some of the people who had their personal information exposed. One person asked not to be contacted again. Another declined to comment and a third person said she was "scared" and was being "cautious." The Public Press reporter for this story was also affected by the data breach.

RansomHub, the attacker of Patelco, was one of the top ransomware hackers last year, according to the FBI's 2024 Internet Crime Report (https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf) . Last year, the U.S. saw $16.6 billion in reported losses from internet crime, a 33% increase from the previous year. Data breaches were among the most frequent complaints to the agency.

As they become increasingly commonplace, data breaches remain a serious problem for consumers.

If someone with bad intentions gets hold of your personal information, including your driver's license number and Social Security number, that person can commit crimes using your name, said Brian Hofer (https://secure-justice.org/hofer-bio) , executive director of Oakland nonprofit Secure Justice and former chair of Oakland's Privacy Advisory Commission. For consumers with exposed personal data, especially when it is posted on the dark web, "the potential harm is enormous" and "unlimited," Hofer said in an interview.

Stolen personal information can be sold on the dark web for pennies on the dollar and "because the same data can be sold over and over and over, it's likely to be in the hands of more people than via a commercial service" selling personal information like LexisNexis, Hofer wrote in an email.

Hofer said he suffered from identity theft himself a few years ago and it took him three years to get his credit report cleaned up because of the many fraudulent entries and fake accounts opened in his name.

A lot of the personal information found in data breaches is already publicly accessible for many U.S. consumers, but each subsequent breach adds a bit to a person's digital profile — or footprint — and brings additional context to their lives, explained Pegah K. Parsi (https://www.linkedin.com/in/pegahparsi/) , chief privacy officer for the University of California, San Diego. The first instance of a breach of someone's Social Security number or driver's license number may be the most significant, but "each additional one still matters," she wrote in an email.

California's Department of Financial Protection and Innovation fined Patelco $100,000 through a consent order (https://dfpi.ca.gov/wp-content/uploads/2025/02/Consent-Order-Patelco-Credit-Union.pdf) in February and ordered the credit union improve its cybersecurity systems and practices. Patelco has paid the penalty and submitted an action plan and quarterly progress report to improve its cybersecurity, agency spokesperson Daniel Emmons (https://www.linkedin.com/in/daniel-emmons-519b0922/) wrote in an email.

The U.S. legal and regulatory landscape does a mediocre job of holding institutions accountable, Parsi wrote, adding that most companies still view privacy through the lens of risk to the organization rather than risk to the individual. This leaves consumers at "greater and greater risk" as more and more of their data is collected, used, bought and sold, she wrote.

This could also lead to organizations taking consumer risk less seriously and arguing that, "'It's already out there so no big deal or bad press to the org if more is then leaked,'" Parsi wrote.

When asked to comment, Patelco spokesman Brian Davis wrote that "we don't have anything to add" and would not answer questions about the class action case or the effects of the data breach on account holders.

Patelco was established in 1936 by employees from the Pacific Telephone and Telegraph Company, which later became AT&T. According to Patelco's 2024 annual report, the credit union has $9.4 billion in assets and close to 500,000 members nationwide. The company operates 36 branches in and around Sacramento and the greater Bay Area, including two in San Francisco.

The U.S. government urges companies to take proactive measures to safeguard their systems and data from ransomware, explained Cybersecurity and Infrastructure Security Agency spokesperson Marci McCarthy (https://www.linkedin.com/in/marcimccarthy/) . Essential cybersecurity practices include enabling multifactor authentication, enforcing strong passwords, keeping software updated and training employees to recognize and avoid phishing attempts, she wrote in an email.

McCarthy advised that for consumers whose data has been compromised in a breach, it is crucial that they closely monitor their accounts and credit reports and report any suspicious activity immediately to authorities (https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Protecting_Sensitive_and_Personal_Information_from_Ransomware-Caused_Data_Breaches-508C.pdf) .

Get our email newsletter

Don't miss out on our newest articles, episodes and events!

Email address SIGN UP