Guess Fashion Brand Deals With Data Loss After Ransomware Attack

By Becky Bracken

Published: 2021-07-13 · Archived: 2026-04-05 13:47:00 UTC

An attack on Guess compromised the personal and banking data of 1,300 victims.

A February ransomware attack on fashion label Guess linked to Colonial Pipeline attackers DarkSide is still causing damage. Guess has started sending letters to 1,300 employees and contractors who had their personal and banking data exposed during the breach.

The letter, published by BleepingComputer, offers victims a year of free credit monitoring and identity theft protection. But it's Guess's breach notification filing with Maine's Attorney General's Office that said more than 1,300 people had their information compromised during the ransomware attack, including account numbers, debit- and credit-card numbers, and even the related security codes, access codes and personal identification numbers.

Guess said the leaked data was discovered during a forensic examination of the attack, which was completed on June 3.

"The information accessed or acquired may have included your Social-Security number, driver's-license number, passport number, and/or financial account number," the letter read.

Employees and Contractors Exposed

Guess director of public relations, Kaitlyn Quail, later clarified it wasn't customers of the retailer who had their information compromised, rather what she called a "subset of employees and contractors whose information was involved."

At the time of the ransomware attack, the group DarkSide bragged it had stolen more than 200 GB of data from the mall stalwart. They even included a professional recommendation about the best way to pay the ransom.

"We recommend using your insurance, which just covers this case. It will bring you four times more than you spend on acquiring such a valuable experience," DataBreaches.net reported in April.

The group's audacity led them to attack the U.S. Colonial Pipeline later, after which their DarkSide operations were interrupted, and their servers and funds confiscated.

The fallout threat to the victims stemming from the Guess ransomware attack will remain for years to come, according to Uriel Maimon with PerimeterX.

"When hackers obtain information from a breach, both the company and it's customers can be affected for years to come," Maimon said via email. "Personal information, for example, can be used to create synthetic identities that are then used to generate fraudulent credit card or loan applications which inevitably affects the original users but also the financial institution."

Guess Breach 'Extremely Valuable' Dataset

The incredibly sensitive nature of the breached data would be valuable to anyone looking to steal identities, according to Erich Kron with KnowBe4.

"Although the Darkside ransomware group is out of commission, that does not mean this breach is insignificant," Kron told Threatpost. "The significant amount and very personal types of data being collected by the organization, including passport numbers, Social-Security numbers, driver's-license numbers, financial account and/or credit/debit-card numbers with security codes, passwords or PIN numbers, is an extremely valuable dataset for cybercriminals if they want to steal identities. "

He cautioned organizations to avoid storing this type of data for long periods of time.

Dirk Schrader with New Net Technologies was a bit harsher in his criticism of Guess and said he's going to be on the lookout for the Security and Exchange Commission to get involved.

"There is a fairly large number of unanswered questions in this breach notification and the event itself," Schrader told Threatpost. "Why sensitive personal information like SSNs or account details was stored in clear text is one of them. Being stock-listed, it will be interesting to read through filings for additional details and whether SEC will ask for more details."

Check out our free upcoming live and on-demand webinar events – unique, dynamic discussions with cybersecurity experts and the Threatpost community.
