Fashion retailer Guess discloses data breach after ransomware attack

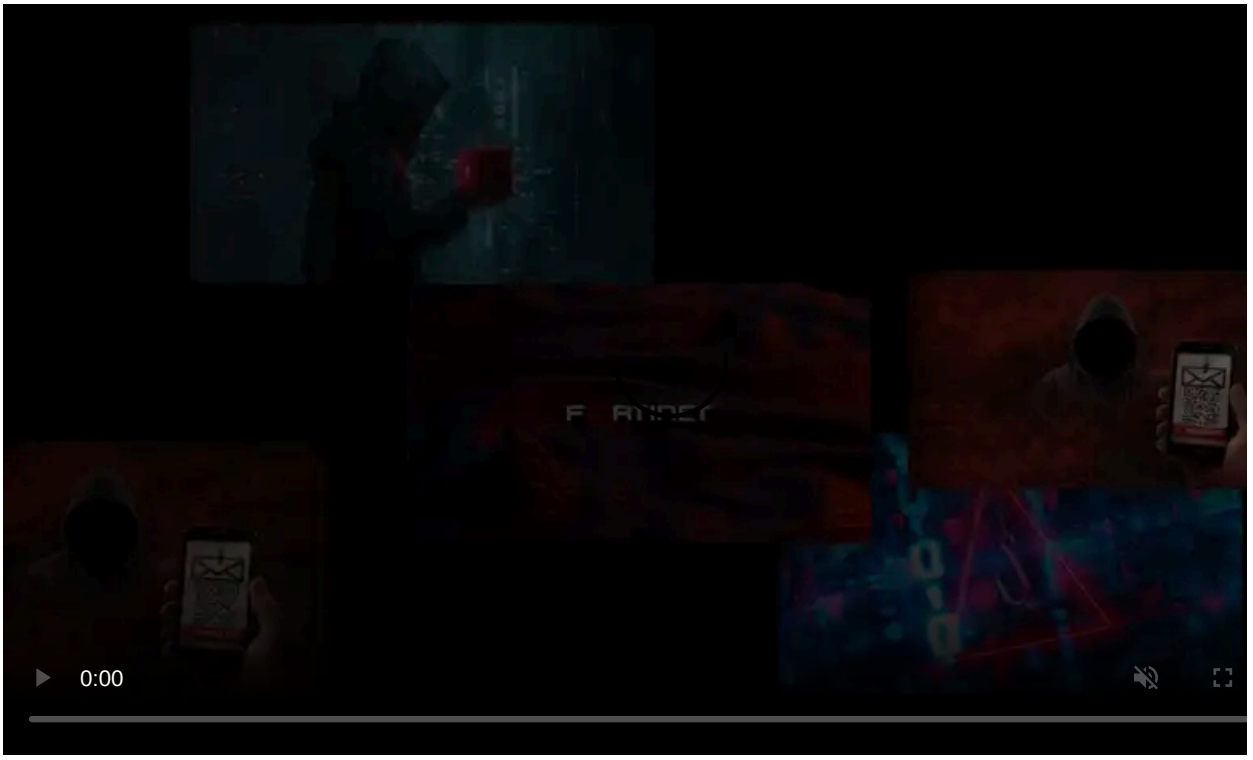
By Sergiu Gatlan

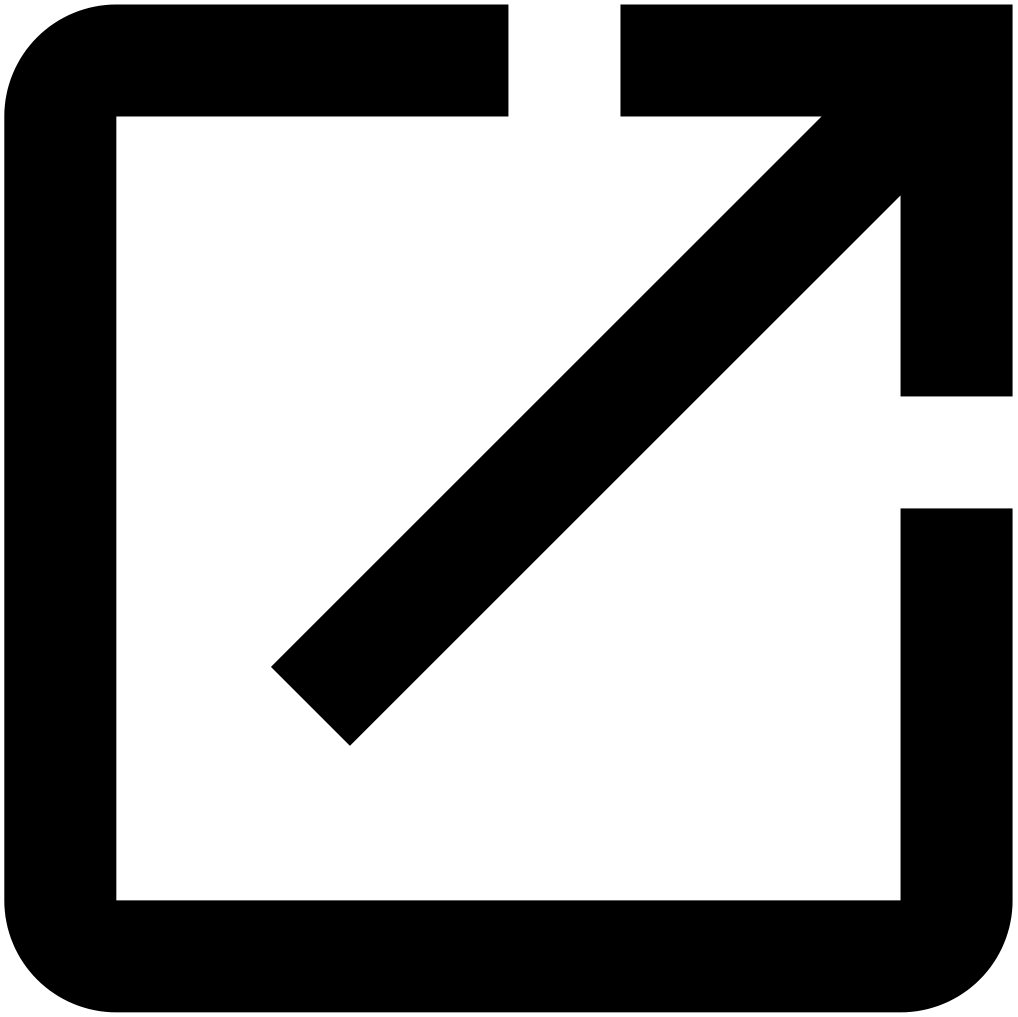
Published: 2021-07-12 · Archived: 2026-04-05 23:13:29 UTC

American fashion brand and retailer Guess is notifying affected customers of a data breach following a February ransomware attack that led to data theft.

"A cybersecurity forensic firm was engaged to assist with the investigation and identified unauthorized access to Guess' systems between February 2, 2021 and February 23, 2021," the company said in breach notification letters mailed to impacted customers.

"On May 26, 2021, the investigation determined that personal information related to certain individuals may have been accessed or acquired by an unauthorized actor."


0:00



Guess directly operates 1,041 retail stores in the Americas, Europe, and Asia, and its distributors and partners another 539 additional stores worldwide as of May 2021. The stores part of Guess' retail network currently operate in roughly 100 countries around the world.

Personal and financial info stolen in the attack

The fashion retailer identified the addresses of all impacted individuals after completing a full review of the documents stored on breached systems on June 3, 2021.

Guess began mailing breach notification letters to affected customers on June 9, offering complimentary identity theft protection services and one year of free credit monitoring through Experian to all impacted individuals.

According to the breach notifications mailed on Friday, information exposed in the attack includes personal and fin

"On May 26, 2021, the investigation determined that personal information related to certain individuals may have been accessed or acquired by an unauthorized actor," Guess said.

"The investigation determined that Social Security numbers, driver's license numbers, passport numbers and/or financial account numbers may have been accessed or acquired."

While the breach notification letters do not reveal the number of affected individuals, information filed with the office of Maine's Attorney General shows that just over 1,300 people had their data exposed or accessed during the February attack.

The filed breach info also reveals that the information acquired during the incident includes "Financial Account Number or Credit/Debit Card Number (in combination with security code, access code, password or PIN for the account)."

Guess has implemented additional measures to boost its security protocols and is cooperating with law enforcement as part of an ongoing incident investigation.

DarkSide ransomware likely behind the attack

Even though Guess did not provide any info on the identity of the threat actor behind the ransomware attack, DataBreaches.net reported in April that the DarkSide ransomware gang listed Guess on their data leak site.

At the time, the ransomware group claimed to have stolen over 200 GB worth of files from the fashion retailer's network before attempting to encrypt their systems.

DarkSide has been active since at least August 2020, focusing on corporate networks and asking millions of dollars for decryptors and the promise not to leak the stolen data online.

The ransomware gang landed in the crosshairs of US law enforcement after taking down Colonial Pipeline, the largest fuel pipeline in the US, in May.

After heightened scrutiny from law enforcement and having some of their infrastructure seized or brought down, DarkSide suddenly shut down in late May, allegedly out of fear of being arrested.

Update: When asked to confirm the identity of the threat actors behind the incident, Guess' Director of Public Relations Kaitlyn Quail sent BleepingComputer the following statement after the article was published:

> Guess?, Inc. recently concluded an investigation into a security incident that involved unauthorized access to certain systems on Guess?, Inc.'s network. We engaged independent cybersecurity firms to assist in the investigation, notified law enforcement, notified the subset of employees and contractors whose information was involved and took steps to enhance the security of our systems. The investigation determined that no customer payment card information was involved. This incident did not have a material impact on our operations or financial results.

Source: https://www.bleepingcomputer.com/news/security/fashion-retailer-guess-discloses-data-breach-after-ransomware-attack/