Acer settles online breach probe for $115k

Article status notice: This Article's Relevance Is Under Review

This article has been flagged for **questionable relevance**. Its connection to the systemic consumer protection issues outlined in the Mission statement and Moderator Guidelines isn't clear.

If you believe this notice has been placed in error, or once you have made the required improvements, please visit the Moderators' noticeboard or the `#appeals` *channel on our Discord server: Join Here.*

Notice: This Article's Relevance Is Under Review

To justify the relevance of this article:

- Provide evidence demonstrating how the issue reflects broader consumer exploitation (e.g., systemic patterns, recurring incidents, or related company policies).
- Link the problem to modern forms of consumer protection concerns, such as privacy violations, barriers to repair, or ownership rights.

If you believe this notice has been placed in error, or once you have made the required improvements, please visit either the Moderator's noticeboard, or the `#appeals` channel on our Discord server: Join Here.

Acer agreed to pay $115,000 and reform its data security practices after a year-long lapse exposed the personal and financial information of more than 35,000 customers.[1][2] The New York Attorney General's office found that Acer left its U.S. website misconfigured and in debugging mode, allowing attackers to access unencrypted credit card details and other sensitive data between 2015 and 2016.

Background [edit | edit source]

Acer is a Taiwan-based electronics manufacturer best known for producing computers, laptops, and related hardware. Its products are sold globally through various retail channels, including its U.S. online store, acer.com. At the time of the incident, Acer relied on this platform for direct-to-consumer sales, making the security of its website critical for handling sensitive customer data, including payment card transactions.

Breach [edit | edit source]

The breach began when Acer's U.S. e-commerce platform was improperly managed between July 2015 and April 2016. An employee had enabled debugging mode, which stored customer data in plain text log files including: names, full credit card details, addresses, and login credentials. In addition, the website was misconfigured to allow directory browsing, enabling attackers to easily access subdirectories and extract sensitive files. Between November 2015 and April 2016, attackers made

attackers to easily access subdirectories and extract sensitive files. Between November 2015 and April 2016, attackers made hundreds of unauthorized data requests, ultimately stealing the information of 35,071 individuals. The breach first came to light in January 2016, when Discover Card flagged Acer as a common point of purchase in fraudulent transactions.

Acer's response [edit | edit source]

According to the customer notice letter submitted to the California Attorney General's office:[3]

- Notification: Acer sent a formal *Notice of Data Breach* to impacted customers, informing them that if they shopped on the Acer e-commerce site between May 12, 2015 and April 28, 2016, their personal and payment information may have been exposed, including name, address, credit card number (with the last digits specified), expiration date, and CVV security code. Acer clarified the hackers did not collect Social Security numbers, and they had no evidence that passwords or login credentials were compromised California DOJ Attorney General. It should be noted that in the settlement with the New York State Attorney General, Acer admitted username and passwords were part of the breach. [1]
- Remediation Actions: Acer stated that it took immediate steps to remediate the security issue upon discovery and enlisted outside cybersecurity experts to assist, though details on those steps were lacking. It reported the incident to its credit card payment processor and offered full cooperation to federal law enforcement California DOJ Attorney General.
- Consumer Guidance Offered: The notice included a Resources Guide advising customers to monitor their account statements, watch for signs of identity theft or fraud, and take proactive steps such as:
  - Reviewing their free annual credit reports (via annualcreditreport.com),
  - Filing a police report if they suspect identity theft,
  - Contacting the Federal Trade Commission or their State Attorney General's office for assistance,
  - Placing fraud alerts and security freezes with national credit reporting agencies, Equifax, Experian, and Transunion.
- Acer offered a toll-free number for customer questions.

Settlement with New York State Attorney General [edit | edit source]

In January 2017, Acer reached a settlement with the New York Attorney General's office, agreeing to pay $115,000 in penalties and adopt a range of security reforms.[1] These included designating employees to oversee data protection, implementing annual staff training, adopting multi-factor authentication, deploying intrusion detection systems, and conducting regular penetration tests and vulnerability assessments. Acer also committed to following credit card industry data security standards and to hold service providers to the same level of compliance.

Consumer response [edit | edit source]

Consumers expressed frustration, distrust, and tangible harm following Acer's data breach. On HardForum, several posters reported that they never received a notification from Acer despite being affected, and some discovered fraudulent charges on their credit cards after purchasing through Acer's online store.[4] Others criticized Acer for mishandling sensitive payment data, particularly for storing CVV codes, which violates standard payment card security rules. The overall tone was one of anger at both the breach and Acer's poor communication.

On The Register's forum, reactions were similarly skeptical and critical.[5] Commenters condemned Acer for failing to follow PCI DSS compliance standards and for allowing card verification codes to be compromised.[6] Some users confirmed they did receive breach notification letters, though experiences varied widely. Many expressed concern that Acer's negligence would push costs and risks onto consumers through fraudulent charges and credit monitoring needs.

Consumers faced heightened risks of identity theft and financial fraud due to the exposure of full credit card details, login credentials, and personal addresses. The fact that sensitive data was stored unencrypted in plain text worsened concerns about Acer's handling of private information. While the settlement imposed stronger protections going forward, many customers were left to deal with potential fraudulent charges, credit monitoring, and long-term distrust in Acer's ability to safeguard their personal information. Public statements from the Attorney General emphasized consumer expectations for companies to uphold basic data security standards, reflecting broader frustration with corporate negligence in protecting private data.[1]

private data.

References [edit | edit source]

1. ↑ 1.0 1.1 1.2 1.3 Schneiderman, Eric (2017-01-26). "A.G. Schneiderman Announces Settlement With Computer Manufacturer After Data Breach Exposed More Than 35,000 Credit Card Numbers" . *New York State Attorney General's Press Releases*. Retrieved 2025-08-18.
2. ↑ Mlot, Stepanie (2017-01-27). "Acer Settles Online Breach Probe for $115k". *PC Mag*. Retrieved 2025-08-18.
3. ↑ Acer's Notice of Breach to Customers https://oag.ca.gov/system/files/Customer%20Notice%20Letter%20-%20California_0.pdf?
4. ↑ "Acer Admits Hackers Stole Up To 34,000 Customer Credit Cards". *[H]ardForum*. 2016-06-20. Retrieved 2025-08-18. {{cite web}}: |first= missing |last= (help)
5. ↑ Nichols, Shaun (2016-06-17). "You Acer holes! PC maker leaks payment cards in e-store hack". *The Register*. Retrieved 2025-08-18.
6. ↑ Pasher, Justin (2016-06-17). "Re: Storing CC security verification codes". *Forum on 'The Register'*. Retrieved 2025-08-18.

Categories: CS1 errors: missing name | Articles marked as irrelevant | Acer