COLORTOKENS

# Timeline of U.S. Retail Cyberattacks and Data Breaches in 2020

The retail industry has been the target of cyberattacks more than any other sector for three years in a row.[1] Capturing customer email addresses, credit card numbers, and even birthdates can net cybercriminals large financial rewards on the Dark Web. Here are some noteworthy retail industry cyberattacks and data breaches from 2020.

## January

### Hanna Andersson

Children's clothing retailer Hanna Andersson reported it had been victimized by a cyberattack in late 2019. Hackers installed malware in the chain's third-party e-commerce platform to collect and sell customer data: payment card numbers, CVV codes, and both billing and shipping addresses.[2]

## March

### Walgreens

Walgreens, the second largest pharmacy chain in the U.S., announced an error within their mobile app's messaging feature that exposed not only personal messages sent within the app, but also customer names and prescription details.[3]

### J. Crew

Clothing retailer J. Crew announced that it had been hacked in April 2019. Personally identifying information (PII) including names, the last four digits of credit card numbers, expiration dates, and billing addresses were accessed, although details of how the breach occurred were not released.[4]

## April

### Quidd

Nearly 4 million login records from online marketplace Quidd, likely stolen in 2019, were found posted on a public hacker forum. User names, hashed passwords, and email accounts were shared among members.[5]

## June

### Claire's

Jewelry and accessories retailer Claire's was victimized by a Magecart cyberattack that deployed a payment card skimmer and collected data from an unknown number of customers.[6]

JAN
FEB
MAR
APR
MAY
JUN
JUL
AUG
SEP
OCT
NOV
DEC

## July

### Drizly

Online alcohol delivery startup Drizly disclosed to customers that a hacker accessed details of 2.5 million accounts. The customer information exposed included email addresses, birthdates, and hashed passwords.[7]

## September

### Staples

Around 2,500 customers of office supply giant Staples received email notifications disclosing their information was exposed in a data breach. The data included names, addresses, email addresses, phone numbers, and last four payment card digits.[8]

## October

### Barnes & Noble

Famous bookseller Barnes & Noble confirmed a cyberattack that took Nook online services offline, with users unable to access their libraries. Customer email addresses, billing and shipping addresses, phone numbers, and transaction histories may have been exposed during the breach.[9]

## November

### JM Bullion

Magecart malware embedded in the online shopping platform of precious metals dealer JM Bullion captured the personal and payment card information of customers who made purchases between February and July.[10]

[1] https://www.trustwave.com/en-us/resources/library/documents/2020-trustwave-global-security-report/
[2] https://www.bizjournals.com/portland/news/2020/01/22/hack-exposes-retailers-customer-data.html
[3] https://healthitsecurity.com/news/walgreens-reports-data-breach-from-personal-mobile-messaging-app-error
[4] https://securityboulevard.com/2020/03/data-breach-u-s-retailer-j-crew-reveals-2019-security-incident-to-customers/
[5] https://www.zdnet.com/article/account-details-for-4-million-quidd-users-shared-on-hacking-forum/
[6] https://www.helpnetsecurity.com/2020/06/15/magecart-claires-intersport/
[7] https://techcrunch.com/2020/07/28/drizly-data-breach/
[8] https://securityboulevard.com/2020/09/staples-discloses-data-breach-exposing-limited-customer-information/
[9] https://www.zdnet.com/article/barnes-noble-confirms-cyberattack-customer-data-breach/
[10] https://www.bleepingcomputer.com/news/security/gold-seller-jm-bullion-hacked-to-steal-customers-credit-cards/