COLORTOKENS

Timeline of
Global Finance Cyberattacks and Data Breaches in 2020

The finance industry typically outspends other sectors when it comes to cybersecurity investments,[1] but hackers still manage to find vulnerabilities. As banking, financial, and insurance institutions increase their digital services portfolios to serve their tech-savvy customers, their threat surfaces also increase. Here are some of the biggest cyberattacks and data breaches that the financial sector experienced in 2020.[10]

January

Travelex – United Kingdom

Currency exchange website Travelex shut down its systems following a REvil cyberattack. Major banks such as Barclays, Lloyds, and RBS were affected by the downtime since they use Travelex for exchange services. The REvil ransomware group demanded a USD $6 million ransom in exchange for providing the decryption key and deleting stolen customer data.[2,3]

February

Nedbank – South Africa

Nedbank, one of South Africa's biggest banks, reported a security breach in a third-party service provider's network that exposed the personal data of 1.7 million customers. The breach did not spread to the bank's system, but the hacker accessed names, identity numbers, addresses, and phone numbers.[4]

March

Robinhood – United States of America

California-based trading platform Robinhood suffered multiple outages leaving its 10 million clients unable to trade equities, options, or cryptocurrency. Some clients took to social media claiming to pull out funds, and these posts claimed over 8,000 followers, damaging the firm's reputation.[5]

Finastra – England

London-based financial technology company Finastra was attacked by ransomware that affected thousands of its servers. Finastra did not disclose details about the breach's impact, but reports say the company's core business suffered outages for several days.[6]

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

August

Experian – South Africa

The South African unit of consumer credit reporting company Experian experienced a data breach that allegedly exposed personal data of 24 million customers and nearly 800,000 local businesses. Investigations show that the suspect had intended to sell the information as marketing data to insurance and credit-related companies.[7]

September

BancoEstado – Chile

One of Chile's biggest banks shut all branches following a ransomware attack. Investigators believe that an employee received and clicked on a malicious document that installed a backdoor on BancoEstado's network.[8]

KuCoin – Singapore

The Singapore-headquartered cryptocurrency exchange KuCoin disclosed a hack that wiped out about $150 million from its funds. Bitcoin, ERC-20, and other tokens in KuCoin's hot wallets were transferred out of the exchange.[9]

November

Liquid – United States of America

Customers of Liquid, a crypto trading platform, were asked to change login credentials after the company was hacked in a domain name hosting attack. The breach exposed emails, names, addresses, and encrypted passwords of customers.[10]

[1]https://cybersecurityventures.com/cybersecurity-market-report/
[2]https://www.cshub.com/attacks/articles/incident-of-the-week-ransomware-hits-currency-dealer-travelex
[3]https://www.infosecurity-magazine.com/news/travelex-forced-administration/
[4]https://www.zdnet.com/article/nedbank-says-1-7-million-customers-impacted-by-breach-at-third-party-provider/
[5]https://www.cnbc.com/2020/03/27/robinhoods-offer-to-traders-impacted-by-outage-come-with-a-catch.html
[6]https://www.cshub.com/attacks/articles/incident-of-the-week-finastras-ransomware-attack
[7]https://www.zdnet.com/article/experian-south-africa-discloses-data-breach-impacting-24-million-customers/
[8]https://www.zdnet.com/article/chilean-bank-shuts-down-all-branches-following-ransomware-attack/
[9]https://www.tribuneindia.com/news/science-technology/over-150-million-emptied-in-kucoin-cryptocurrency-exchange-hack-147430
[10]https://techcrunch.com/2020/11/18/cryptocurrency-exchange-liquid-confirms-hack/