



CA\$H APP DATA BREACH

Understanding the Breach, Its Impact, and Lessons Learned

INTRODUCTION

What is Cash App?

- A mobile payment service by Block, Inc. (formerly Square)
- Used for peer-to-peer payments, investing, and more

Why Data Security Matters:

- Fintech platforms handle sensitive financial data
- Breaches can lead to financial loss and loss of trust

Purpose of This Presentation:

- To analyze the Cash App breach, its causes, and its implications

WHAT HAPPENED

Timeline:

- Breach occurred: December 2021
- Disclosed: April 2022

Key Details:

- Former employee downloaded internal reports
- 8.2 million Cash App Investing users affected
- Data exposed: Names, brokerage account numbers, portfolio values

HOW DID IT HAPPEN

Insider Threat:

Former employee retained access after leaving

Access Control Failure:

Lack of proper revocation of access

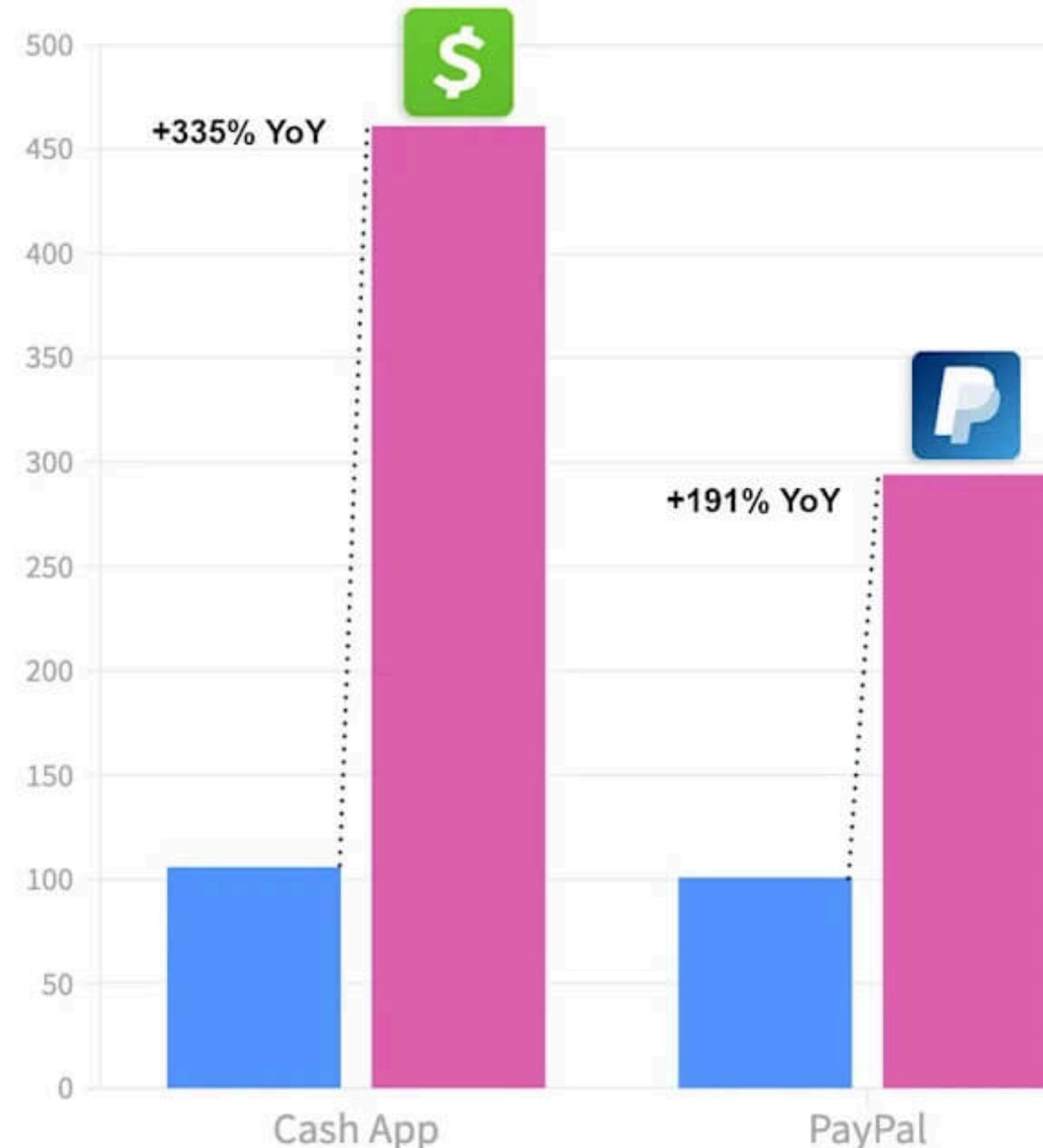


SCAMS AND FRAUDS!

Payment apps struggle to get scammers under control

Total mentions of "fraud" or "scam" in app user reviews

February 2020 February 2021



apptopia

SCAMS AND FRAUDS!



Shania Jensen @shania_jensen · Mar 7

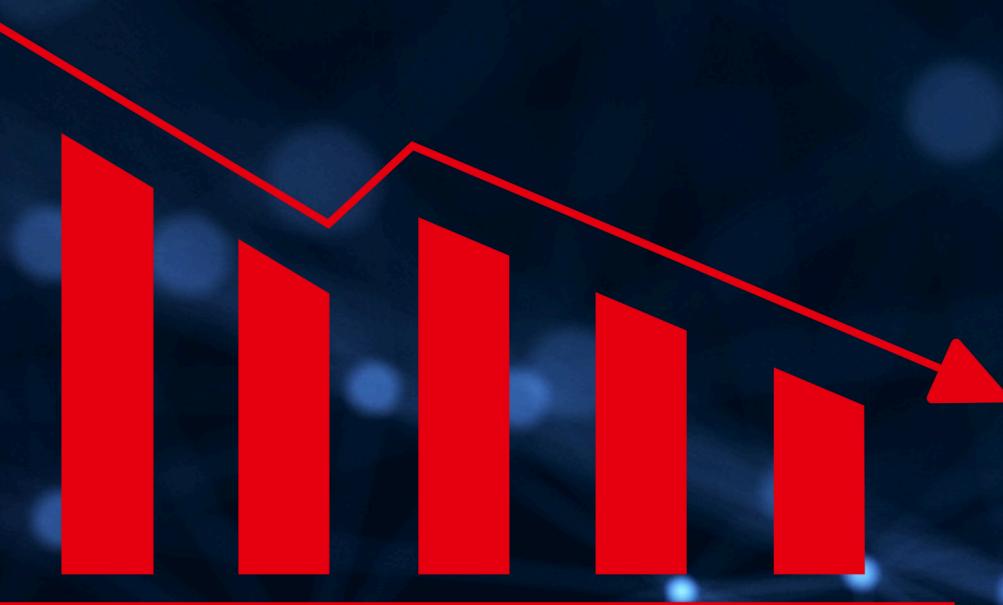
Woke up to every dollar to my name stolen and hacked out of my account in the middle of the night! @CashApp @CashSupport @jack can't feed my kids today because I have ZERO dollars. And somehow the cash support cannot even email or call back! This is not ethical and not okay!

The screenshot shows a list of failed transfer attempts:

- Devon** At 12:00 AM: \$500 (Failed)
- Changhyun** (grid icon): \$2,624 (Failed)
- Michael Foley** (grid icon): \$2,600 (Failed)

At the bottom of the screen are standard social media interaction icons: a speech bubble with '2', a retweet icon with '2', a heart with '3', and an upward arrow.

IMPACT OF THE BREACH



On Customers:

Risk of phishing and identity theft
Loss of trust in Cash App



On Block, Inc.:

Regulatory scrutiny
Reputational damage

On the Industry:

Increased focus on insider threats and data minimization

COMPANY RESPONSE

Block, Inc.'s Statement:

Notified affected customers

Reported to regulators (SEC)

Claimed no financial data or passwords were exposed

Actions Taken:

Investigated the breach

Strengthened access controls

KEEPING USERS

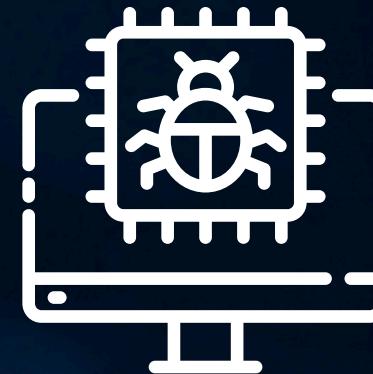


Cash App customers can claim up to \$2,500 in class-action settlement

LEASONS LEARNED

Insider Threat Mitigation:

Implement strict access controls



Data Minimization:

Limit access to sensitive data

Timely Disclosure:

Notify affected parties promptly



Employee Training:

Educate employees on data security



CONCLUSION

Recap:

The Cash App breach highlights the risks of insider threats and the importance of data security

Key Takeaways:

Insider threats are a major risk

Proactive measures are essential to protect customer data

Call to Action:

Companies must prioritize cybersecurity to prevent future breaches

MEASURES!

Zero-Trust Security:

Verify all access requests

Automated Tools:

Monitor and revoke access automatically

Compliance:

Ensure adherence to data protection laws (GDPR, CCPA)

Proactive Measures:

Regularly audit security practices

**THANK YOU FOR
ATTENTION**