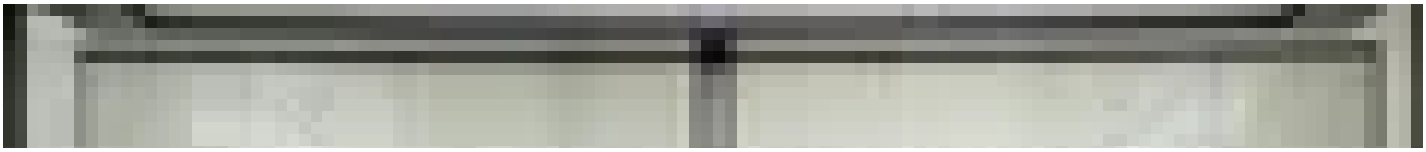
Four Indicted in Massive JP Morgan Chase Hack

The four defendants netted hundreds of millions of dollars in stock-pump scheme and internet gambling operations, Feds say.



FEDERAL AUTHORITIES HAVE indicted four men on charges that they hacked into multiple financial institutions and operated a stock-pumping scheme and online gambling operations that netted them more than 100 million dollars.

The Feds say the defendants are responsible for hacking into JP Morgan Chase last year and obtaining access to more than 80 million customer accounts.

Authorities have charged Gery Shalon, Joshua Samuel Aaron, and Ziv Orenstein on 23 counts, including unauthorized access of computers, identity theft, securities and wire fraud and money laundering. The fourth hacker who helped them breach the networks has not been identified.

The US District's Office in Atlanta, Georgia also announced additional separate charges against Shalon, Aaron, and an unidentified hacker—the indictment in Georgia charges ten counts including unauthorized access of computers and wire fraud. Orenstein is only being charged in New York.

In addition to breaching JP Morgan Chase, they are charged with hacking into six other financial institutions, as well as financial news sites, online stock brokers and even software companies. Dow Jones, the parent company of the *Wall Street Journal*, was among those hacked, as were Scottrade and ETrade.

"The massive scale of these data breaches is staggering," said John Horn, the US Attorney in Atlanta.

The unidentified hacker used multiple methods to break into the networks, including brute-force attacks. At one point, Aaron also tricked a victim in the US into providing login credentials to ETrade and Scottrade networks. The hacker then used this access to locate customer databases on the networks.

Notably, one of the vulnerabilities the hackers used to obtain access to sites was the Heartbleed vulnerability discovered and exposed last year.

The operation, allegedly led by Shalon, ran from 2012 to 2015 and ultimately led to the theft of more than 100 million victims' data.

The defendants stole customer information because they were hoping to establish their own brokerage business, according to online chats between the perpetrators that authorities obtained. They spoke about modeling Merrill Lynch's business practices to build their business, but with stolen customer data to give them a leg up.

The hackers breached JP Morgan in 2014. At the time it was reported that the intruders compromised data on 76 million personal accounts and more than 7 million small business accounts.

According to documents filed with the Securities and Exchange Commission, JP Morgan asserted that only names, addresses, and emails were taken in the breach. The attackers weren't able to steal money, credit card numbers, passwords, or social security numbers.

Yet that information proved to be lucrative enough to bring the attackers a big payday. The thieves allegedly operated a stock price manipulation scheme that let them amass millions of dollars. They also operated a dozen illegal internet gambling sites and a Bitcoin exchange that generated millions more, according to authorities.

The attackers "relied for their success on computer hacking and other cybercrimes," according to authorities.

To hide their activities they set up dozens of shell companies and used fake passports and other fraudulent credentials to maintain false identities.

Kim Zetter is an award-winning, senior staff reporter at Wired covering cybercrime, privacy, and

security. She is writing a book about Stuxnet, a digital weapon that was designed to sabotage Iran's nuclear program.