

CORRECTED-UPDATE 3-Security breach hits U.S. card processors, banks

Fri Mar 30, 2012 7:37pm EDT

- * Visa, MasterCard, American Express, Discover hit
- * Breach stems from third-party Global Payments
- * Unclear how many accounts affected

By [Lauren Tara LaCapra](#) and Carrick Mollenkamp

March 30 (Reuters) - Four giant card-payment processors and large U.S. banks that issue debit and credit cards were hit by a data-security breach after third-party services provider Global Payments Inc discovered its systems were compromised by unauthorized access.

It was not immediately clear how many cardholders became victims of the breach, which affected MasterCard Inc, Visa Inc, American Express Co and Discover Financial Services, as well as banks and other franchises that issue cards bearing their logos.

U.S. law enforcement authorities including the Secret Service are investigating and MasterCard said it has hired an independent data-security organization to review the incident.

The shares of Atlanta-based Global Payments, which acts as a credit-checking middleman between merchants and card processors, were halted on Friday afternoon after dropping more than 9 percent on the news.

MasterCard shares fell 1.8 percent to close at \$420.54, Visa shares dropped 0.8 percent to \$118, American Express shares fell 0.1 percent to \$57.86, while Discover rose 1.2 percent to \$33.34.

Analysts said any financial losses from the data breach would be shouldered by merchants, card issuers and Global Payments rather than Visa or Mastercard, which operate payment networks.

Global Payments said it determined that an unauthorized entity had accessed its systems and possible customer card data in early March. Krebs on Security, a blog that first reported the incident on Friday, said accounts had been compromised for over a month, between Jan. 21, 2012 and Feb. 25, 2012.

Global Payments is holding an investor conference call Monday morning to discuss the issue.

This Global Payments breach is just the latest in a long string of incidents that have put the personal information of millions of credit and debit cardholders at risk.

Individual banks and processors said they had not yet determined the full extent of the breach, but Krebs on Security described it as a "massive" breach that may affect more than 10 million cardholders.

Some industry experts suggested the figure might be much less, perhaps on the order of tens of thousands. Bernstein Research analyst Rod Bourgeois noted that Global Payments is a relatively small player in the transactions services industry, servicing 800,000 merchants with a 3.5 percent market share. By contrast, the largest competitor, First Data, services millions of merchants, with 22.6 percent of the market.

JPMorgan Chase & Co, as well as American Express and Discover, which issue their own cards, said they are monitoring customers' accounts and would issue new cards to anyone whose information may have been compromised.

Citigroup Inc said it has been notified by processors of the breach. Bank of America Corp declined to comment on the matter and Wells Fargo & Co said it was too early to comment on the impact.

Banks and processors emphasized customers would not be held liable for any fraudulent charges that may occur.

Mike Simonsen, the Chief Executive of real-estate research company Altos Research, said he may have been a victim.

Simonsen said he was contacted by his bank, Bank of America Corp, last week about his Visa card. Although there were no unauthorized transactions, the representative told him a vendor or law enforcement agency had flagged his account as compromised and so he would receive a new one.

"It was very unusual," he said.

PROCESSING PIPELINE

Global Payments, which has about 3,700 employees, was spun off from information-services firm National Data Corp in 2001. For the fiscal year ended May 31, Global Payment reported revenue of \$1.9 billion, an increase of 13 percent from the year-earlier period. According to a company presentation in January, the company was projected to report fiscal 2012 revenue in the range of \$2.15 billion.

The company is scheduled to report fiscal third-quarter results on Wednesday and there had been the expectation Global Payments would report improving results. On Wednesday, Sterne Agee raised its price target for Global Payments to \$65 a share from \$58.

Global Payments is one of dozens of companies that operate along the payment-processing chain, between the time a person swipes a card to pay and the time the payment is delivered.

The account number, expiration date and possibly the cardholder's name is sent from the point of payment to a processor, which then connects to Visa, MasterCard, American Express or Discover. Information is then sent to the card issuer - often a bank - which ultimately authorizes the transaction.

The actual transfer of money occurs later.

Processing companies, which perform millions of authorizations each day, are supposed to encrypt card information. But a breach could occur if someone gains access to the system and identifies a gap in the encryption.

The information that was likely collected illegally from Global Payments is called Track 1 and Track 2 data. A person improperly using the information can transfer the account number and expiration date to a magnetic strip on a card and then try to use the card on a website.

Thousands of U.S. banks that issue credit and debit cards receive daily alerts regarding breaches through a system referred to as CAMS, said Thomas McCrohan, an analyst with Janney Capital Markets.

The illegal use of the data could be stymied if an online merchant asks for the three or four digits printed on a card known as the "CVV code."

"The systems can all be made tighter, but if they're too tight no transactions would ever be approved," said Edward Lawrence, a director at Auriemma Consulting Group, a payment systems consultant. "You still have to allow commerce to occur."

Rep. Mary Bono, a California Republican who chairs the House Subcommittee on Commerce, Manufacturing and Trade, condemned the Global Payments breach and urged Congress to adopt stronger data-security legislation this year.

"You shouldn't have to cross your fingers and whisper a prayer when you type in a credit card number on your computer and hit 'enter,'" she said in a statement.

RIPPLE EFFECTS

The Visa-Mastercard-Discover breach is the first major instance this year of consumer information put at risk by technological flaws or hacking, but there are plenty of examples of massive data breaches in recent years affecting banks, retailers, technology companies and payment processors.

Last June, Citigroup said computer hackers breached the bank's network and accessed data of about 200,000 cardholders in North America.

Sony Corp also reported several recent attacks, including one last year in which hackers accessed the personal information on 77 million PlayStation Network accounts.

Google Inc suffered a major attack on its Gmail accounts in 2011 that it said appeared to originate in [China](#). Attacks against Gmail users involved direct attempts to compromise accounts by tricking users into revealing information - so-called "phishing" - or by gathering their passwords from other websites, rather than compromising Google systems, according to the company.

Separately, TJX Companies Inc and Heartland Payment Systems Inc have had their systems compromised.

On Friday, retailers were already beginning to look for fraudulent purchases from the compromised card accounts stemming from the Global Payments breach. They will bear the financial brunt of those crimes under rules worked out with the card associations and issuers, analysts said.

"Our merchant community is sitting here girding itself and looking at their own fraud-prevention strategies and bracing for the influx of bad transactions," said Tom Donlea, managing director for the Americas at the nonprofit Merchant Risk Council. "After Heartland and after the Sony breach, there was an increase in fraud activity."