Blue Cross Blue Shield Blue Care Network of Michigan **News**

Stephanie Beres
313-549-9884 newsroom@bcbsm.com

Blue Cross Blue Shield of Michigan investigators aid law enforcement officials in arrests for identity theft carried out in southeastern Michigan

BCBSM begins process of notifying 5,514 affected members

DETROIT, March 10, 2015 – Corporate investigators from Blue Cross Blue Shield of Michigan played an active role in a federal law enforcement investigation resulting in the arrests today of 11 individuals in southeastern Michigan for alleged identity theft.

The arrested individuals possessed the personal information of 5,514 Blue Care Network and Blue Cross Blue Shield of Michigan members in printouts captured from the companies' information systems. A former employee of BCBSM was among those arrested.

"We are pleased that assistance provided by our company's investigative team was used to secure the arrest of these individuals, including our former employee," said Daniel J. Loepp, president and CEO of BCBSM. "I am personally saddened by this former employee's involvement. Their alleged behavior in no way represents the ethical standards brought to work every day by our more than 7,000 employees, who are committed to serving our members with integrity and honesty."

Affected members will be contacted by letter and offered two years of free credit protection services. To further protect their personal information, BCBSM recommends members carefully monitor their Explanation of Benefits statements and financial accounts for services they did not receive or any inappropriate or suspicious healthcare claims. In the event that they notice any inappropriate activity on their Explanation of Benefits statements, BCBSM and BCN ask members to contact the companies' Anti-Fraud Hotline at 800-482-3787, between 8:30 a.m. and 4:30 p.m. Monday through Friday.

"Blue Cross and BCN are committed to protecting our members' personal information," said Kevin Klobucar, CEO for Blue Care Network. "We have taken a number of deliberate steps to further secure our members' information from disclosure, including limiting access to members' Social Security numbers, requiring all employees to change their passwords, and installing new printing devices that require employees to scan their coded badges to print."

# # #