Extracted from *Law360*:

Biggest-Ever Hacking Bust Restores Faith In DOJ

Law360, New York (July 26, 2013, 8:33 PM ET) -- In charging five Eastern European men with hacking their way to hundreds of millions of dollars, federal prosecutors on Thursday finally demonstrated a desire and ability to unravel complex international cyberattacks, a welcome display for companies that have long sought a stronger government response to the barrage of data breaches they face.

According to **indictments unsealed** in New Jersey and New York, the five defendants allegedly conspired with others to penetrate the computer networks of Nasdaq, Heartland Payment Systems Inc., Dow Jones & Co. Inc., the Jordanian arm of Visa Inc., J.C. Penney Co. Inc. and a dozen other payment processing companies, retailers and financial institutions, leading to the theft of more than 160 million credit card numbers and millions of dollars in losses for the alleged corporate victims.

Federal officials from the U.S. attorney's office for New Jersey, the U.S. Department of Justice and the U.S. Secret Service pointed to the crucial role that international cooperation and authorities' technological sophistication played in taking down the ring, which employed complex techniques that allowed hackers to set up camp in corporate systems undetected for years and lift data that was stored in an array of computers located around the world.

Federal officials' willingness to pool their resources to identify and prosecute individuals associated with sophisticated international hacking operations is likely to provide great comfort to the scores of businesses that are increasingly being targeted by these attacks, attorneys told Law360 on Friday.

“In this age of increasing cyberattacks, any efforts along these lines to apprehend and publicize the charging of cybercriminals is welcomed by corporate America,” said Alexander H. Southwell, co-chair of the information technology and data privacy group at Gibson Dunn & Crutcher LLP and a former cybercrimes prosecutor. “Oftentimes, turning to law enforcement is the only thing that a company can do because they don't have the resources or capabilities of reaching abroad to go after somebody.”

While many companies report cyberintrusions to law enforcement officials because of their breach notification obligations or internal best practices, they often question whether officials have the time, capabilities or interest to pursue attacks from an unknown source that is accessing corporate servers from outside the U.S., according to Alston & Bird LLP partner and former federal prosecutor Kim Peretti.

But the indictment unsealed Thursday — which targets what federal officials called the largest identity theft ring ever prosecuted in the U.S. — removes much of that doubt, she said.

“It certainly gives companies encouragement that law enforcement will pursue a case if there is significant access to their systems, even if a person is outside the country and the case may not have been pursued in previous years,” she said.

The charges also demonstrate the benefits that can come out of working closely with law enforcement following a breach, helping to calm fears that sharing information with the government will lead to an automatic punishment for having weak internal safeguards, according to attorneys.

“Increasingly, companies recognize that their resources alone are insufficient to repel the resourcefulness of hackers, particularly those who collaborate in an extensive, worldwide scheme as alleged here,” said Fernando M. Pinguelo, chairman of the cybersecurity and data protection and crisis management groups at Scarinci Hollenbeck LLC. “Therefore, there is often a benefit to participating in outreach programs … whereby information and resources are shared with the common goal of putting an end to the invasion.”

The advantages of working with the government are more visible now than ever, given that officials are making cybersecurity a priority and have built a robust network of international collaborators in recent years, according to Peretti.

“The investigation suggests that in the right case, law enforcement now has the sophistication, the experience and the resources to be able to investigate serious international hacks,” Weisbrod Matteis & Copley PLLC partner and former DOJ computer crime division attorney Peter Toren said. “If they have people that are competent and able to investigate computer crimes, that makes it more appealing for hacking victims to work with law enforcement to investigate attacks.”

Law enforcement's more aggressive pursuit of hackers may also act as a deterrent to future attacks, according to attorneys.

“The fact that these charges have been brought for attacks that happened a number of years ago ... indicates the persistence that law enforcement has and should send a message to cyberattackers that they will continue to be hunted long after their attacks have faded off the front page,” Southwell said.

The case could also help block hackers by encouraging companies to tighten their data security protections, given the indictments' suggestion that the hackers went undetected in the companies' systems for years, according to McKenna Long & Aldridge LLP partner and former federal prosecutor Ray Aghaian.

“Companies need to realize that cyberattacks are a big problem, and hopefully indictments like these will push companies to take steps to better secure their systems,” he said. “That way, attacks can be discovered sooner and criminals will be able to profit a lot less.”

But other attorneys doubted that one case would be enough to make any significant impact on the growing tide of sophisticated cyberattacks.

“The 'take' is too high, egos too big, feelings of invincibility too rampant to discourage such behavior,” Pinguelo said. “The fact that two of the accused here [Alexandr Kalinin and Vladimir Drinkman] were also charged in 2009, in the then-largest data breach ever reported, [of Heartland Payment Systems,] just goes to show how recidivism is rampant.”

Still, attorneys predict that this action is just the first in many to come from federal prosecutors.

“Hacking and computer crimes are now at the forefront of what is happening at a daily basis, and it's now the FBI's top concern, so I think the government is going to place a lot more emphasis on investigating and prosecuting these types of cases,” Aghaian said.

The cases unsealed Thursday are U.S. v. Vladimir Drinkman et al., case No. 09-cr-00626, in the U.S. District Court for the District of New Jersey; and U.S. v. Nikolay Nasenkov, case No. 09-cr-01093, in the U.S. District Court for the Southern District of New York.