

Chairman Weisz and members of the committee,

My name is Marc Wallman. I serve as Vice President for Information Technology at North Dakota State University. I am here today to report on the status of the security attack at NDSU related to targeted phishing emails. The incident in question resulted in seven employees having their August 29, 2014, paychecks deposited into bank accounts that did not belong to them.

I would like to begin with some background information. The University System, including NDSU, use Microsoft Office 365 for email and calendar. Office 365 is a Microsoft-hosted solution that provides email, calendar, instant messaging and other services. The ConnectND HR/Finance systems are hosted by the state IT Department and managed by the North Dakota University System's Core Technology Services department. As the HR/Finance systems are not under my direction, my comments will focus on activities at NDSU. However, I would like to acknowledge that both NDUS CTS and ITD were excellent partners in working to assess the cause and scope of this incident.

In the months of August and September, a phishing attack aimed at stealing employees' paychecks was targeted at research universities in the United States. On August 12, 2014, people at NDSU received phishing emails related to this scheme. The number of recipients of known variants of the email exceeded 50. The phishing email included a website link, which pointed to a site hosted by a Russian Internet Service Provider (ISP). The ISP has since taken down the site. The website accurately mimicked the design of an NDSU website. This scheme was first reported to NDSU HR/Payroll on August 13. On that same day, NDSU HR/Payroll sent an alert to NDSU employees notifying them of this scheme.

On August 28, an NDSU employee happened to notice that her direct deposit information had been reset to a bank that was not hers. She contacted NDSU HR/Payroll who **(1)** corrected this before her paycheck was sent to this bank, **(2)** alerted the Bank of North Dakota and **(3)** ran a report in ConnectND to search for other employees who had their routing/account numbers reset to this bank. They found none.

On September 2, another NDSU employee contacted NDSU HR/Payroll because his pay was not directly deposited into his bank account. NDSU HR/Payroll worked with Core Technology Services staff to develop a new tool to identify all NDSU employees who recently had their direct deposit information reset. Eight employees were identified as being affected. Seven of these employees had their paychecks deposited into bank accounts that weren't theirs. The incident was reported to NDSU Police who have been working with the FBI to investigate this issue.

NDSU IT security officers scanned the university-owned computers of all affected employees. No malware was discovered on any of the computers. Network traffic logs were analyzed to determine which computers and users at NDSU had connected to the phishing website. Approximately 50 people were identified as having visited the website. All were contacted and asked to change their ConnectND passwords. Network logs indicate some, but not all, of the people affected by the direct deposit attack visited the phishing website.

Subsequent to this incident, NDSU system administrators checked our servers and applications to ensure this attack was not the result of password harvesting from a server or system at NDSU. The checks all came back clean: None of our systems were compromised, and no passwords were harvested from NDSU servers or applications.

This concludes my prepared remarks. I am happy to answer any questions the committee may have.

October 30, 2014