Data Incident Response - UPDATED

November 25, 2019
Naviance

This is an updated response notification. The updated information is in **bold** below.

Montgomery County Public Schools (MCPS) is notifying you of a data security incident that occurred with Naviance, an online college and career readiness program that supports MCPS students in exploring and developing their postsecondary plans. **During further investigation of a data security incident impacting Naviance accounts at Wheaton High School, MCPS, in collaboration with the Montgomery County Police Department (MCPD), determined that the individual responsible for the incident at Wheaton High School also accessed and downloaded information from students' Naviance accounts at five additional MCPS schools. The schools impacted include: Wheaton High School, Montgomery Blair High School, Julius West Middle School, Argyle Middle School, Parkland Middle School, and A. Mario Loiederman Middle School.**

MCPS is committed to safeguarding the privacy and security of our students, families, and staff and MCPS sincerely regrets that this incident has occurred. MCPS takes this event very seriously and has implemented improvements to prevent such unauthorized access from happening again. Additional information regarding this data security incident is provided below. We will continue to be forthcoming with any relevant information.

What Happened?

Naviance notified MCPS on October 4, 2019 that a data security incident occurred on October 3, 2019 impacting 1,343 Naviance student accounts and one parent/guardian account at Wheaton High School. An unauthorized user performed a brute force attack against Wheaton High School's Naviance platform in order to access user accounts. The unauthorized user attempted many username and password combinations, eventually gaining access to 1,344 accounts. The unauthorized user then downloaded demographic information from the accessed accounts. Naviance immediately reset passwords for the affected users. For details regarding Wheaton High School, please refer to the initial Data Incident Response.

As noted in the initial Data Incident Response, MCPS and MCPD successfully identified a student to be responsible for the brute force attack and MCPD took possession of the student's devices (a laptop and an iPhone) for further investigation.

On November 6, 2019, MCPD notified MCPS that they had completed a forensics analysis of the student's devices and that they found evidence of additional attacks performed by the student against multiple MCPS Naviance platforms between September 12, 2019 and September 14, 2019. After further investigation, MCPS and MCPD determined that the student accessed a total of 5,962 accounts across six schools. The student downloaded the same demographic information that was downloaded from the Wheaton High School accounts. The information accessed did not include social security numbers, banking information, or credit card information. At this time, MCPD does not believe that the student shared any accessed information with others. The student currently faces additional disciplinary action based on the expanded scope of the brute force attacks as well as possible criminal charges.

When MCPS learned of the attacks against the multiple MCPS Naviance platforms between September 12, 2019 and September 14, 2019, MCPS immediately contacted Naviance and confirmed that the additional accounts were accessed by the student.

What Information Was Involved?

The following chart describes the data elements that were exposed:

Exposed Data Elements		
Name	Date of Birth	Highest ACT Score
Ethnicity	Grade Level	Highest IB Score
Gender	Student ID #	Student Address
GPA	Weighted GPA	Home Phone #
Email Address	Highest SAT Score	Mobile Phone #
Assigned Counselor	Highest PSAT Score	Nickname

What We Are Doing

Previously, as part of the response to the Wheaton High School data security incident, MCPS forced a district-wide password reset for all Naviance student accounts to prevent any further unauthorized access. **By resetting all student passwords at that time, the accounts impacted by the attacks between September 12, 2019 and September 14, 2019 were also secured from further unauthorized access.**

What You Can Do

As with any incident regarding personally identifiable information, there are many precautionary steps that parents/guardians can take to secure their child's identity. Recommendations include the following:

- Request a free credit freeze for your child. A credit freeze will make it difficult for someone to use your child's information to open accounts. To place a freeze, follow the specific instructions from each of these credit bureaus: Equifax, Experian, and TransUnion.
- Check to see if your child has a credit report. Each bureau listed above has specific instructions for these requests. If a credit bureau has a credit report for your child, the credit bureau will send you a copy of the report. Use the instructions provided with the credit report to remove the fraudulent accounts.
- Review information on Child Identity Theft from the Federal Trade Commission.

For More Information

If you have any questions regarding this incident, or if you desire any further information or assistance, please email information_security@mcpsmd.net.