# ME, MY .ORG, AND AI

## Scenario 2: Preventing Fraud: Artificial Intelligence and Nonprofits

***Instructions:*** *Take the next 2 - 3 mins to read through the following scenario quietly on your own. Once finished, there are a series of questions for you to consider, first on your own and then with your group. At the end of your discussion, be prepared to report back to the group about what you have discussed with your breakout room.*

___________________________________________________________________

In January of this year, Ed4U – an education non-profit specializing in providing online schooling to rural communities across Central America – was the victim of fraud. $500,000 USD was stolen from their accounts. A malicious agent hacked Marco, a project manager's laptop; she had passwords and details pertaining to their online bank accounts saved as a word document on her hard-drive. The hacker emptied her department's account within hours of infecting her laptop with malware.

Fraud investigators found that the hacker had attempted to access a number of devices in Ed4U's network. The malware that attacked Marco's device was sent through email: the hacker posed as another non-profit inviting her to checkout a list of foundations currently offering funding to nonprofits.

Furious over the loss of programming that the fraud has caused, Ed4U's sponsors and supporters are pushing for Ed4U to update their financial systems. One foundation has even withdrawn funding over concerns that systems and funds are being "mismanaged". Devastated and embarrassed, Marco has spearheaded the push for a fraud-prevention specialist to speak to all the project managers across Ed4U.

At the Fraud prevention workshop, Sammi – the specialist – explains the difference between human and non-human weaknesses. They detail the ways in which human behavior can damage the integrity and safety of the entire network. These behaviors include: not regularly changing your password, saving confidential information on a laptop or other device without any encryption, not leaving devices unlocked in public spaces, not sharing passwords with colleagues or friends/family, and not sharing devices with colleagues or family/friends.

When they explain non-human weaknesses, Sammi describes how malware is growing increasingly powerful and capable of breaching firewalls, encryption, and other protections. She presents them with a short list of the pros and cons of using big tech companies versus smaller, boutique firms' private servers. Though there are ethical and safety concerns on both sides of the spectrum, ultimately, big companies have better resources to design, implement, and safeguard their cloud and other private servers.  AI solutions, they go on, can be used to enhance security across a number of business sectors, from retail to the nonprofit sector. They carefully explain how it can help monitor corporate Ed4U card usage and device or endpoint access.

This leads Marco to ask about the specific data storage that Ed4U uses: raises a number of concerns about privacy and data storage: where is the data collected? Who has access to the information? Sammi confirms that Ed4U's admits that the data is stored on private servers – namely, the BigCo cloud, but that the benefits of AI outweigh the ambiguities she just outlined. Using AI means more effectively linking points of compromise and preventing fraud at Ed4U. AI can analyze the behaviors of transactions and devices so that it can detect unfamiliar and malicious behavior early, preventing loss of funds and other breaches.

Sammi reassures Ed4U that companies such as MasterCard and RBS WorldPay have relied on AI to detect fraudulent transaction patterns and prevent card fraud for years now. However, they cannot provide additional clarity on how data is stored or how it is used by the service provider outside of fraud detection.

**Prompt questions: Use your remaining time to think through the following questions, alone or together in a group.**

Question 1 & 2: **On your own, take two mins to consider the following 2 questions. Feel free to jot down notes on a separate sheet of paper.**

- What might **your** org's board/leadership need to be prepared for a situation like this?
- What human vulnerabilities (regarding digital security) are at play within **your** organization?  Which ones do you think you should you prioritize?

Question 3: **Group Activity - in your small groups, fill out the following table.**

- Take 2 minutes to identify pros and cons of using AI -powered cloud storage for your organization.
- Focus specifically on potential harms (list in column 3) and whom those harms hit hardest (service beneficiaries, staff, etc.) - **See the table below**

| Pros | Cons | Potential Harms | To whom? |
|---|---|---|---|

| | | | |
|---|---|---|---|
| | | • Monitoring/Privacy<br>• Reputational harm<br>• Decline in funding and services | • Employees (when organizations are using monitoring systems)<br>• Everybody your organization works with (the community/anybody who partners with the organization)<br>• Other organizations in that space (chilling effect that erodes trust)<br>• Reputational and financial harm to the organization |
| | | | |

**<u>As a group be prepared to report out to the whole:</u>**

- Who do you think is most harmed by data breaches?
- What does that mean for how your organizations should act?
- What can you do as individual organizations or collectively to mitigate the harms?