Q&A - For Stores to Communicate to Customers

What Happened?
The <INSERT STORE NAME> recently learned that PrismRBS, a vendor that provides our eCommerce website, experienced a security incident in which an unauthorized party was able to gain access to and install malicious software designed to capture payment card information on some of the eCommerce servers that host <INSERT STORE URL>.

What data was affected?
Based on the forensic investigation, it appears that the unauthorized party was able to access payment card information, including cardholder names, card numbers, expiration dates, card verification codes and billing address for certain transactions made on the website.

Because we do not collect sensitive information such as Social Security, passport or driver's license numbers, this type of information was not affected by this incident.

What about purchases made on other websites or at other venues on campus?

This incident affected only eCommerce transactions made on <INSERT STORE URL> between January 19th and January 26th, 2019; transactions made outside of this period of time, those made in our on-campus facility and other university transactions were not affected by this incident.

What about transactions paid for using financial aid?
For customers using financial aid as their payment type, the only sensitive information that may have been affected would be name, student ID number and shipping address.

What we (the bookstore) are doing?
Our website provider has engaged a PCI validated forensics data company to conduct a comprehensive investigation. Additionally the vendor has implemented several additional security measures to help prevent this type of incident from reoccurring in the future.

Is the bookstore offering credit monitoring services?
As an added precautionary measure, we are offering **one year** of identity protection services through IdentityWorks. Call 877-239-1287 for instructions on how to take advantage of this service.

What you (the customer) can do?

- You can review your credit or debit card account statements to determine if there are any discrepancies or unusual activity listed.
- Remain vigilant and continue to monitor statements for unusual activity going forward.
- If you see something you do not recognize, immediately notify your financial institution as well as the proper law enforcement authorities.

- In instances of credit or debit card fraud, it is important to note that cardholders are not typically responsible for any fraudulent activity that is reported in a timely fashion.
- Social Security numbers and other sensitive personal information were not at risk in this incident. As a good general practice, it is recommend that you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate.
- If you see anything you do not understand, call the credit agency immediately.
- As an additional precaution, the letter you received included an "Information about Identity Theft Protection" reference guide, which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection.

Q&A - For Stores to Communicate to Campus Partners/Leadership

What is PrismRBS doing to address this incident?

1. PrismRBS initiated an IT Computer Security Incident Response Team and followed standard processes for a security event.
2. PrismRBS informed their entire customer base on January 26th.
3. PrismRBS engaged with a 3rd party PCI certified Forensic Investigation Team.
4. PrismRBS provided live monitoring of all affected systems throughout the duration of the investigation.
5. PrismRBS is providing us with information and resources to aid in the process of contacting our affected customers (end-users).
6. **PrismRBS will make a summary of the investigation findings available upon request.**

Has PrismRBS alerted credit card companies?

PrismRBS, as a service provider, is following all legal and PCI council mandated reporting requirements which includes notification of the card companies.

Do we need to alert state officials?

The regulations differ state by state. We have engaged the Information Security department on campus to confirm if we need to notify the state attorney general's office.