Alright everyone, thank you for joining this important kick-off call for our annual PCI DSS audit, version 4.0. This is a crucial process to ensure the security of our customers' payment card data and maintain their trust in our e-commerce platform. Let's get started by addressing these key questions:

Who in your organization has access to the cardholder data?

Within our organization, access to cardholder data is strictly limited based on job function and the principle of least privilege. Primarily, the following teams and roles may have access, depending on the specific data element and system:

- **Customer Service:** Certain members of our customer service team may access masked cardholder data (e.g., last four digits) for transaction verification and support purposes. Access is logged and monitored.
- **Payment Processing Team:** A small, dedicated team within our finance department handles payment reconciliation, reporting, and exception processing. They have access to the necessary data to perform these functions.
- **IT and Security Teams:** Select members of our IT and security teams have access to systems that store, process, or transmit cardholder data for maintenance, monitoring, and security purposes. Their access is role-based and regularly reviewed.
- **Management:** Limited members of senior management have oversight access for reporting and strategic decision-making.

It's important to emphasize that direct, unmasked cardholder data access is highly restricted and auditable. We maintain strict access controls and regularly review user permissions.

Do you know which systems are in scope for PCI DSS?

Yes, we have a preliminary understanding of the systems in scope for PCI DSS. Based on our initial assessment, the following are likely to be included:

- Our e-commerce website and its underlying infrastructure.
- The payment gateway integration components.
- The servers and databases that store, process, or transmit cardholder data, even in an encrypted format.
- Any network segments that connect to these systems.
- Related logging and monitoring systems.

We will be working closely with the IT team and our Qualified Security Assessor (QSA) to finalize the scope and create a comprehensive inventory of all in-scope systems.

Does your website take credit card payments directly?

No, our website does not directly handle the processing or storage of sensitive credit card details. We utilize a PCI DSS compliant third-party payment gateway to securely process all online transactions. This significantly reduces our PCI DSS scope and risk.

Can you provide a high-level overview of how your business accepts and processes payments?

When a customer places an order on our website and proceeds to checkout, they are securely redirected to our PCI DSS compliant payment gateway provider. On the gateway's secure environment, the customer enters their payment card details. This information is encrypted and transmitted directly to the payment processor. Our systems receive a transaction token or authorization status from the payment gateway, confirming whether the payment was successful. We do not at any point capture, store, or process the full credit card number on our own servers.

Is the payment page a redirect or an API?

Our payment integration utilizes a **redirect** method. When a customer proceeds to pay, their browser is securely redirected to the payment gateway's hosted payment page. Once the transaction is complete, they are redirected back to our website with the order confirmation.

Are there specific systems, departments, or vendors that you know of that should be in or out of scope?

Based on our current understanding:

- **Likely In-Scope:** As mentioned, our e-commerce platform, the integration with the payment gateway, and associated logging and monitoring systems are definitely in scope.
- **Likely Out-of-Scope:** Our marketing website (separate from the e-commerce platform), internal communication tools, and general employee workstations that do not directly interact with cardholder data should be out of scope.
- **Vendors:** Our primary payment gateway provider is definitely in scope as a service provider handling cardholder data on our behalf. We will need to ensure their PCI DSS compliance. Other vendors who might have incidental access or provide services related to in-scope systems will also need to be assessed.

We need the IT team's input to confirm these initial assumptions and identify any other systems, departments, or vendors that might need to be considered.

How does the company process refunds?

Refunds are initiated through our internal order management system. Authorized personnel within our finance or customer service teams can initiate a refund request. This request is then securely transmitted to our payment gateway provider via API calls. The payment gateway then processes the refund and credits the customer's original payment card. We do not directly access or store the full card details during the refund process; we rely on transaction identifiers provided by the payment gateway.

What are the cloud service providers that are being used?

We currently utilize the following cloud service providers:

- Stripe for our cloud-based payment processing

We need to identify which of these providers host or support any in-scope systems or data and ensure they have appropriate security controls and PCI DSS compliance where applicable.

How do you analyze and identify critical assets, threats, and vulnerabilities within the system?

Our approach to analyzing and identifying critical assets, threats, and vulnerabilities involves several key activities:

- **Asset Inventory:** We maintain an inventory of all hardware, software, and data assets relevant to our e-commerce operations, with a focus on those within the potential PCI DSS scope.
- **Threat Modeling:** We conduct threat modeling exercises to identify potential threats that could impact our critical assets and cardholder data. This includes considering both internal and external threats.
- **Vulnerability Scanning:** We regularly perform vulnerability scans on our external-facing systems, including our website, to identify potential security weaknesses. We also conduct internal vulnerability scans on relevant systems.
- **Penetration Testing:** We engage qualified third-party security experts to conduct periodic penetration testing to simulate real-world attacks and identify exploitable vulnerabilities.
- **Security Monitoring:** We have implemented security monitoring tools and

processes to detect and respond to suspicious activity and potential security incidents.

The IT team plays a crucial role in executing and maintaining these processes.

Can you share what risk assessment methodologies are being used and how do you document the process?

We utilize a risk assessment methodology that aligns with industry best practices and PCI DSS requirements. Our approach typically involves the following steps:

1. **Asset Identification:** Identifying the assets within the scope of the assessment.
2. **Threat Identification:** Identifying potential threats that could impact these assets.
3. **Vulnerability Identification:** Identifying weaknesses in our systems or processes that could be exploited by these threats.
4. **Likelihood Assessment:** Evaluating the probability of a threat exploiting a vulnerability.
5. **Impact Assessment:** Determining the potential business impact if a threat were to successfully exploit a vulnerability.
6. **Risk Calculation:** Combining the likelihood and impact to determine the overall risk level.
7. **Risk Treatment:** Identifying and implementing controls to mitigate, avoid, transfer, or accept the identified risks.
8. **Documentation:** We document the entire risk assessment process, including the identified assets, threats, vulnerabilities, risk levels, and implemented controls. This documentation is regularly reviewed and updated.

We typically use a risk register to track and manage identified risks and their associated mitigation plans.

Who is responsible for maintaining the website and are you aware of whether or not they are trained in secure coding practices?

Our website maintenance is primarily handled by the IT and marketing team. We understand the critical importance of secure coding practices.

- If it's an internal team, we will confirm the training they have received in secure coding principles, such as OWASP Top Ten, and ensure ongoing training is part of their professional development.
- If we utilize an external vendor, we have contractual agreements that require them to adhere to secure coding standards and provide evidence of their developers'

training in this area. We will need to review their security practices and ensure they align with PCI DSS requirements.

Are applications developed in-house and will it be available via mobile app or strictly via website?

Currently, our primary e-commerce application is developed in-house and is accessible strictly via our website. We do not currently have a dedicated mobile application for purchasing. If there are any future plans to develop a mobile app that would handle payment information or interact with in-scope systems, that would significantly impact our PCI DSS scope and require a separate assessment and implementation of security controls from the outset.

Thank you all for your initial input. This information is invaluable as we move forward with our PCI DSS 4.0 audit. The next steps will involve a more detailed technical assessment led by the IT team and our QSA. We encourage open communication and collaboration throughout this process to ensure a successful audit and the continued security of our customer data.