SAMPLE: PLEASE UPDATE WITH YOUR CORRECT BUSINESS INFORMATION AND ENGAGEMENT DETAILS

[COMPANY NAME] Cements Commitment to Keeping Cardholder Data Secure

[COMPANY NAME] recently announced that we underwent a third-party audit to assess our compliance with the Payment Card Industry Data Security Standard (PCI DSS). But what does that mean for us as an organization—and for you as our customer?

At [COMPANY NAME], keeping customer payment card data secure is our top priority. To demonstrate that our systems and controls have been designed appropriately to achieve that goal, we sought an independent assessment from a PCI Qualified Security Assessor (QSA) firm, BARR Advisory.

In this blog post, we'll explain what it means to be PCI DSS compliant and why we chose to undergo this foundational cybersecurity audit.

WHAT IS PCI DSS?

PCI DSS is a globally recognized compliance standard aimed at reducing fraud and safeguarding consumers' payment card information. Developed by major credit card companies, including Visa, Mastercard, and American Express, the standard outlines baseline security requirements for organizations that store, process, or transmit payment card information.

Organizations that interact with cardholder data, or that could impact the security of the cardholder data environment (CDE), must comply with PCI DSS.

WHAT DOES IT TAKE TO ACHIEVE COMPLIANCE?

In order to comply with PCI DSS, organizations must adhere to standards outlined by the PCI Security Standards Council for handling customer credit card data. These standards make up the foundations of a strong cybersecurity program that can effectively manage and mitigate the risk of data breaches.

Those foundations include:

- Building and maintaining a secure network;
- Protecting cardholder data through encryption;
- Implementing strong identity and access controls;
- Maintaining an active vulnerability management program;
- Continuously monitoring network resources, security systems, and processes; and,
- Designing and implementing a comprehensive information security policy.

As our chosen PCI QSA firm, BARR Advisory completed a thorough review of [COMPANY NAME]'s CDE to assess whether we've met these requirements and established effective policies and

procedures for securing cardholder data. The result was a [report of compliance (RoC) / attestation of compliance (AoC) / QSA-assisted self-assessment questionnaire (SAQ)].

WHY DID WE UNDERGO A THIRD-PARTY AUDIT?

Undergoing an independent audit against the PCI DSS framework is a key part of [COMPANY NAME]'s ongoing efforts to demonstrate our commitment to data security and ensure that we're prepared to face the challenges of the ever-changing cybersecurity landscape.

"Demonstrating our compliance against this globally recognized standard helps assure our valued customers and partners that protecting their private data is our top priority," said [COMPANY REPRESENTATIVE NAME, TITLE].

WHERE CAN I GO FOR MORE INFORMATION?

BARR Advisory has published a free downloadable resource explaining all aspects of PCI DSS compliance, including why the standard is crucial for organizations across a variety of industries, changes made in PCI DSS version 4.0, and the steps required for achieving compliance.

Current and prospective customers interested in a copy of [COMPANY NAME]'s [RoC / AoC / SAQ] may contact [NAME] at [PHONE/EMAIL].