

PCI Security Standards Council Bulletin: PCI SSC Impersonation, Phishing, and Know Your Customer (KYC) Scams

13 July 2023

The PCI Security Standards Council (PCI SSC) has learned that one or more unauthorized third parties have been sending communications to or calling PCI stakeholders, including merchants, Community Meeting sponsors and exhibitors, and others, purportedly on behalf of PCI SSC, seeking to elicit financial or other sensitive information and/or potentially sell unauthorized services.

Examples are shown below.

To the extent these or similar communications purport to be from PCI SSC, they are phishing attempts and are illegal.

Although these requests often appear to be from PCI SSC, and in some cases include PCI SSC marks, logos, or contact information, they are not from or endorsed by PCI SSC. These communications may take the following or other forms:

- Emails requesting “Know Your Customer” (KYC) information, “Merchant Member Business Information”, or similar information.
- Emails requesting routing numbers, account numbers, or other sensitive or financial data.
- Email offers for event attendance lists, purporting to be from or associated with PCI SSC.
- Calls from individuals claiming to be PCI SSC representatives offering various services.

PCI SSC will never send industry stakeholders unsolicited requests for routing, account, or similar financial numbers, data, or information.

Some communications have also been purported to be arranging hotel rooms for or providing information about the PCI Community Meetings. We do not work with non-affiliated parties to manage hotel room blocks for these events.

Should you or one of your customers receive unsolicited or unexpected communications purporting to be from PCI SSC and requesting financial or other sensitive data, we strongly encourage you to promptly report the incident to the appropriate authorities in your region.

To confirm information about PCI SSC Community Meetings and other PCI SSC events, all details are available on the [Event](#) page of the website. Questions about information received via email may be directed to pcicm@pcisecuritystandards.org.

PCI SSC publishes resources on defending against common scams and threats. Learn more about [phishing scams](#).

For additional information on reporting scams and fraud in the USA, please see [Report Scams and Frauds | USAGov](#).

EXAMPLE #1:

From: admin@plivo.com <admin@plivo.com>

Sent: Friday, June 30, 2023 8:22 AM

To: [REDACTED]

Subject: KYC REQUIRED

Action Required: Payment Card Industry Compliance

Helping you to keep your merchant account secure is our priority! We would like to remind you that maintaining Payment Card Industry (PCI) compliance is essential to significantly reduce the risk of a data breach at your business.

Dear Valued Merchant,

All merchant members accepting credit/debit card payments are required by the Card Brands (VISA, MasterCard, AMEX, Discover) to be Payment Card Industry Data Security Standard (PCI DSS) compliance. Merchants are required to complete a yearly Know Your Customer (KYC) verification form.

Completed Know Your Customer(KYC) form can be emailed to kycform@pcidss.cc | Completed forms should be sent in before 30th of June 2023, otherwise we would put a temporary funding hold to the merchant processing account.

Thank you for being a valued customer and your continued assistance in contributing to a more secure payment card acceptance environment for all industry members.

THANKS

Risk Department

PCI DSS

kycform@pcidss.cc

PCI DSS Quick Reference Guide

Understanding the Payment Card Industry

Data Security Standard version 3.2.1

For merchants and other entities involved in payment card processing

<https://www.pcisecuritystandards.org/>



PCI Security Standards Council, LLC | 401 Edgewater Place, Suite 600 Wakefield, MA USA 01880 | 218-303-5150

MERCHANT MEMBER BUSINESS INFORMATION

BUSINESS NAME: _____

LOCATION ADDRESS: _____

BUSINESS PHONE: _____

MERCHANT ID(MID): _____

(Duplicate KYC form for more than one MID location)

DIRECT DEPOSIT INFO ON FILE:

ROUTING NUMBER: _____

ACCOUNT NUMBER: _____

SIGNATURE OF AUTHORIZE SIGNER

DATE

PHONE

AUTHORIZE SIGNER NAME

EMAIL ADDRESS



Copyright © 2006 - 2023 PCI Security Standards Council, LLC. All rights reserved. Terms and Conditions.

Association Management services provided by Virtual, Inc. • Antitrust Policy • Privacy Policy • IPR Policy

EXAMPLE #2

From: [REDACTED] <Tactic@tacz-tics.com>

Sent: Thursday, July 6, 2023 8:51 PM

To: [REDACTED]

Subject: PCI SSC Community Meeting 2023

Importance: High

Sensitivity: Personal

Dear Exhibitors,

This is regarding **PCI SSC North America Community Meeting 2023** – Attendees list is available now.

You can use this list for your booth invitation, pre-show marketing campaigns, appointment setting.

Just pick the number that describes best of your response.

- 1. Yes, Send counts & cost.**
- 2. I'm not interested.**

Please Advise

Regards,

[REDACTED] | Marketing Executive

