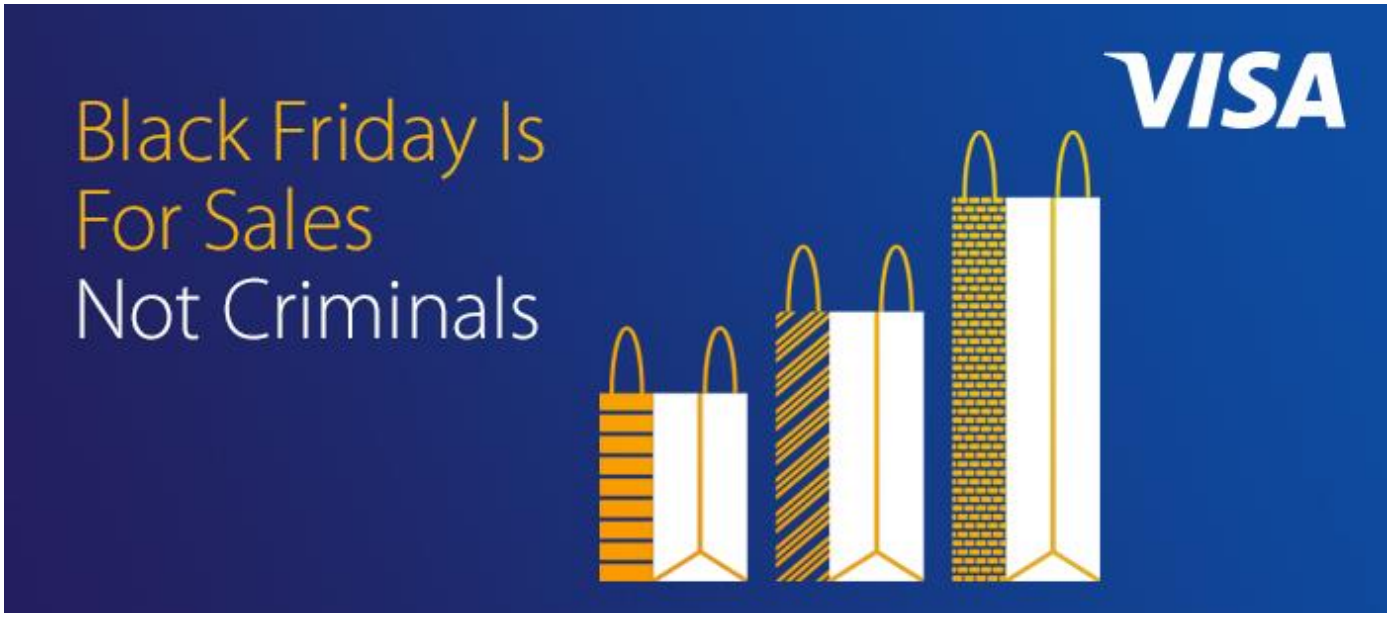

Visa is committed to helping merchants better understand how they can best protect their businesses and customers. As part of this commitment, Visa regularly posts data security alerts on www.visa.com/cisp. These alerts focus primarily on common security vulnerabilities, attack methods, and emerging risks identified in the payment system. Keep your organization informed by accessing alerts, bulletins, and webinars by subscribing to RSS feeds at www.visa.com/cisp.

As the holiday season approaches, Visa is reminding clients, merchants and payment system participants of their responsibility to protect cardholder account and PIN data. Criminals trying to obtain cardholder account and PIN data at the point of sale (POS) frequently target PIN Entry Devices (PEDs) that are known to be vulnerable. In the past, Visa alerted clients to PEDs used in tampering and skimming attacks. All vulnerable PED users are encouraged to upgrade to systems that feature the most up-to-date security.

The Visa material included in this e-mail is targeted to acquirers, processors, merchants, and service providers. It provides guidance for merchants to reduce fraud risk exposure in card-present environments.

ADDITIONAL TRAINING - WEBINAR

STRATEGIES TO EFFECTIVELY MANAGE DATA COMPROMISE EVENTS
WEDNESDAY, 12 NOVEMBER 2014, 10 AM PST

Visa Global Payment System Risk will be hosting a webinar on 12 November 2014 at 10 am PST covering Visa's investigation lifecycle, acquirer and merchant obligations and containment procedures. Please click on the link below to register.

http://visa.adobeconnect.com/risknov2014/event/event_info.html

MORE INFORMATION

If you have any questions regarding these resources or need more information on protecting your payment card environment, please email cisp@visa.com or contact your Visa Account Executive or acquirer.

Other Visa data security webinars can be found at www.visa.com/cisp under the Training tab.

To be removed from Visa Data Security Communications, please reply with “Unsubscribe” in the Subject line.