logo Image not found or type unknown

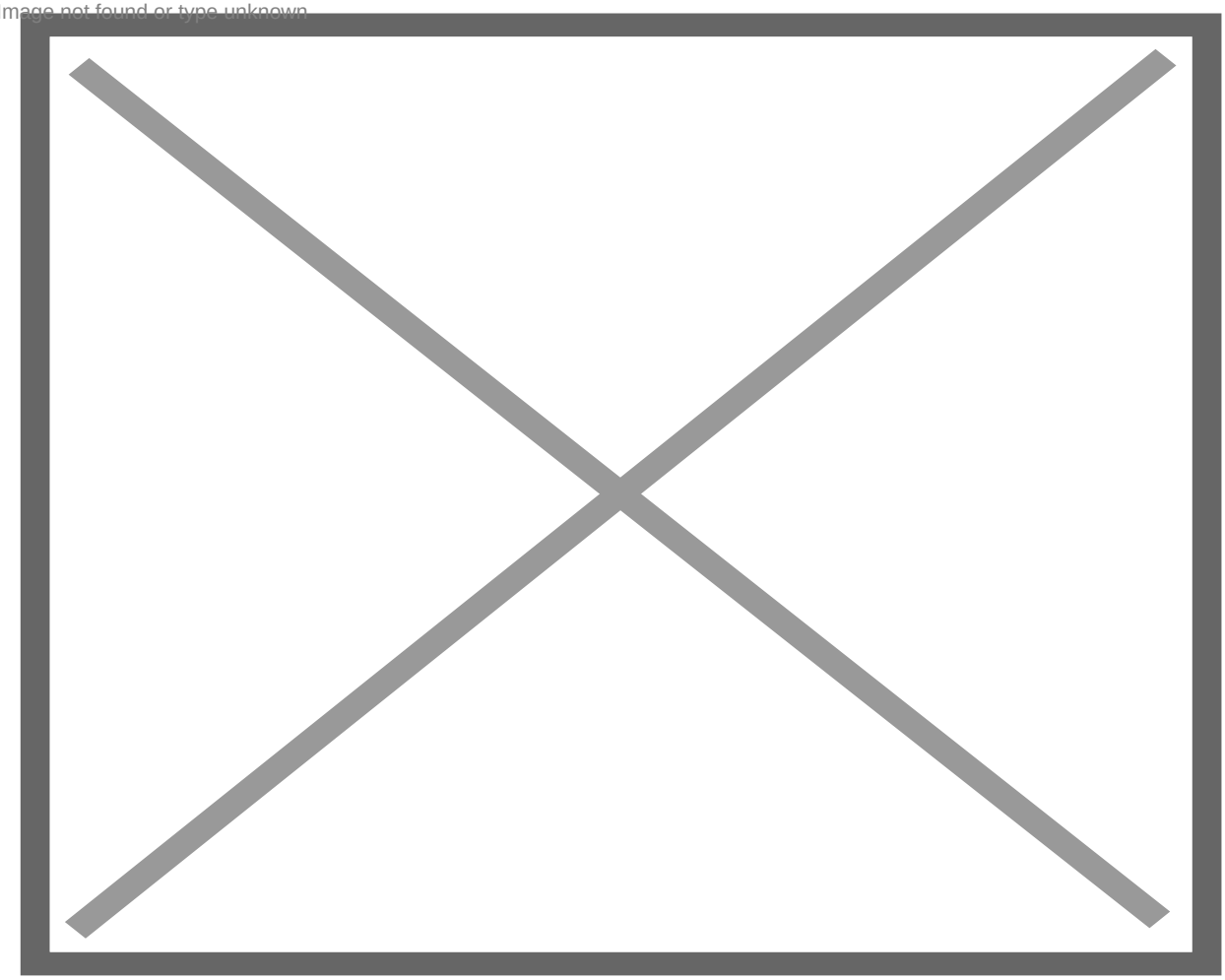
VIPD Warns Local Businesses to Halt Manual Credit Card Entry Amid Rising Fraud Threats

The VIPD is urging businesses to stop manually entering credit card numbers, warning that the practice exposes them to fraud, employee theft, PCI violations, and long-term reputational harm, with multiple cases already under investigation.

Business / **Published On August 04, 2025 02:26 PM /**

Staff Consortium August 04, 2025

Image not found or type unknown



The V.I. Police Department’s Economic Crime Unit is urging businesses across the territory to immediately cease the manual entry of credit card numbers when the physical card is not present. The department emphasized that this outdated practice not only exposes businesses to financial and legal risk but also undermines customer trust and public safety.

The advisory, released on August 4, outlines a series of growing concerns related to fraud, internal theft, and non-compliance with industry regulations. Officials pointed to several ongoing investigations into fraudulent credit card use in the territory, many of which are directly tied to manual data entry practices.

Manual entries, according to the Economic Crime Unit, leave businesses significantly more vulnerable to fraud and identity theft. This vulnerability has already resulted in multiple cases under active investigation.

Beyond the financial impact, there are also serious legal implications. Improper credit card handling can breach Payment Card Industry Data Security Standard (PCI DSS) requirements. Businesses found to be non-compliant may face fines, civil penalties, or even criminal investigations.

The police also highlighted the risk of employee misconduct. Manually entering credit card information can create openings for unscrupulous employees to steal or misuse customer data.

Even a single breach can cause long-term harm to a company's reputation. "Customer trust is critical," the department noted. Businesses that fail to secure transactions may face lasting damage to their public image and consumer relationships.

To help mitigate these risks, the VIPD's Economic Crime Unit issued several clear recommendations:

- Always require a physical card for any in-person transaction.
- Use only secure, PCI-compliant terminals with chip, tap, or swipe capability.
- Provide proper training to all employees on secure card-handling practices.
- Promptly report any suspicious activity by calling 911.

The department closed its notice with a call to collective responsibility: "Let's work together to keep the Virgin Islands safe, secure, and fraud-free."

For further details or to report concerns, businesses are encouraged to contact the VIPD Media Department at vipdmedia1@vipd.vi.gov or visit www.vipd.vi.gov.