VISA SECURITY ALERT **SEPTEMBER 2018**

PURCHASE RETURN FRAUD

DISTRIBUTION: MERCHANTS, ACQUIRERS, PROCESSORS

EXECUTIVE SUMMARY:

Visa Global Payment System Risk is aware of recent incidents in the U.S., in which criminals are committing fraud through processing fraudulent purchase return transactions. As part of the fraud scheme, criminals obtain Point-of-Sale (POS) devices—either from an acquirer or agent while posing as a merchant, from online resellers or auctions, or through theft—and program the POS devices with the credentials of a legitimate merchant, thus effectively cloning the unsuspecting merchant's actual POS device. Criminals subsequently use the cloned POS devices to complete purchase returns to gift cards, often in the range of $2,000 - $6,000 per transaction. After the purchase returns are posted to the gift cards, the cards are cashed out at ATMs. Criminals prefer gift cards, and in certain cases debit cards, as these products often use VisaNet SMS transmission and funds are more rapidly available.

Criminals specifically target merchant credentials and account information, including merchant descriptors, merchant identification numbers (MIDs), or terminal identification numbers (TIDs). Reported methods criminals use to obtain merchant information include collecting transaction receipts showing merchant descriptors, MIDs and sometimes TIDs, scanning used POS device memory slots for applications containing merchant information, or by stealing a merchant's programmed terminal. The criminals possess knowledge of how to program POS device applications and connect such devices to the specific host or front-end platform used by the legitimate merchant.

Threat and Risk Description

Criminals are able to use this fraud scheme to transact high amounts in purchase returns, either to a single card or distributed over various cards. Merchants often do not notice this activity until the funds are deducted from their bank account. If the activity is not detected, suspended or blocked by the acquirer, or subsequently the issuer, the funds are cashed out at ATMs. If the acquirer attempts to reverse the purchase returns after the cash out, the issuer has no recourse for recovering the funds and faces a loss and may request indemnification from the acquirer.

Acquirer Best Practices for Threat Mitigation

1. **Perform Merchant Activity Monitoring**
   - Visa requires that acquirers monitor unusual credit voucher activity. Acquirers should be able to detect credit vouchers that do not have corresponding sale transactions[1].

[1] Effective through 12 April 2019, Visa requires that a merchant must provide a credit refund in connection with a transaction by a credit transaction receipt, which must not be processed without having completed a previous retail Transaction with the same Cardholder

2. **Validate POS Devices**
   - Acquirers and processors should have a manner to validate POS devices that are connected to their host to ensure no unauthorized or cloned POS devices can link to a live MID. Acquirers may consider using a combination of transaction data elements/terminals messages for this validation including, but not limited to the combination of MID+TID+MCC+Descriptor.

3. **Educate Merchants on Good Data Security Practices**
   - Avoid printing sensitive information, such as MIDs or TIDs, on transaction receipts.
   - Remind merchants that account information and terminal applications must be securely deleted from all memory slots when decommissioning a POS device.

4. **Comply with Visa requirements (effective April 2019) to send authorization requests on purchase return transactions.**
   - Visa Business News published in March 2018 includes details on new requirements.

ADDITIONAL RESOURCES:

- Visa's What to Do If Compromised Procedures
- Visa Supplemental Requirements - Visa Global Acquirer Risk Standards