## UNLIMITED OPERATION SCHEMES

The FBI has distributed a Private Industry Notification (PIN 20180809-001) of a global ATM cash-out scheme which cyber criminals have planned to conduct in the coming days.

The planned attacks, referred to as unlimited operations, compromise a financial institution or payment card processor with malware to access bank customer card information and exploit network access, enabling large scale theft of funds from ATMs. Historically, small-to-medium size financial institutions are more susceptible to unlimited operation attacks. The FBI expects this activity to continue or possibly increase in the near future.

## Fraud Attack Method

Unlimited operation attacks are performed by gaining unauthorized network access to accounts at targeted financial institutions. To successfully complete this scheme, criminals need:

1. Unauthorized access to unencrypted bank card data. This may originate from bank customer information, a payment card processor, a point-of-sale vendor or be purchased from another cyber-criminal.

2. The ability to manipulate security and anti-fraud protocols pertaining to:
a. Account balances
b. Withdrawal limits
c. Bank, card and ATM specific security measures

Note: This type of access is typically gained through the financial institutions card management system. Employees should be aware of suspicious emails and not open attachments. This has been an effective method for criminals to gain access to secured systems through key logging and other monitoring methods.

The cyber criminals typically create fraudulent copies of legitimate cards by imprinting stolen card data on reusable magnetic strip cards, such as gift cards. At a pre-determined time, co-conspirators withdraw account funds from ATMs using these cards.

The cyber criminals also alter account balances and security measures to make an unlimited amount of money available at the time of the transactions, allowing for large amounts of cash to be quickly removed from the ATM. Criminals are more likely to initiate this scheme during low visibility times.

The cyber criminals will often launder these funds by converting them into virtual

currency, investing in local or regional criminal enterprises or transferring them overseas. Of note, unlimited operations are distinct from a similar scheme known as "ATM jackpotting" since the software or mechanics of the ATM are not altered to enable the disbursement of funds.

**FBI Recommendations**

Issuers, ISOs and Acquirers should adhere to the following FBI recommendations:

- Implement separation of duties or dual authorization procedures for account balance or withdrawal increases above a specified threshold.
- Implement application whitelisting to block the execution of malware.
- Block execution of files from TEMP directories, from which most phishing malware attempts to execute.
- Monitor, audit and limit administrator and business critical accounts with the required access and authority to modify the account attributes mentioned above.
- Verify the implementation of required security patches.
- Implement real-time monitoring of ATMs activity to ensure that suspicious activities or processes involving ATM software are identified.
- Ensure that Intrusion Detections Systems (IDS) are updated to monitor for the methodology provided in this alert.

Follow network and information security best practices:

- Ensure the security of ATMs and that ATM software is patched and up-to-date.
- Ensure ATMs are operating with the latest version of software.
- Work with the ATM vendors to address overall ATM security.
- Visit the PCI SSC website for more information on security requirements and best practices.
- Keep the software stack and configurations up to date.
- Implement secure ATM installation and software delivery processes.

**Fraud Watch *PLUS***

- In anticipation of potential threats to our clients Fraud Watch PLUS has made

adjustments to existing rule sets to enhance alerting on suspicious activity for both domestic and international ATM transactions.

- Transaction support center is monitoring client ATM activity per normal operations, with focus on cash out schemes
- Fraud Watch Plus On call person will be available for escalation of fraud events

**If you suspect that your financial institution or cardholders have been impacted by an unlimited operation or other type of fraud attack, please immediately call:**

- Support: 1-877-935-2637
    - Technical Support – Option 1
    - ATM Support – Option 2
    - Fraud Support -- Option 4
- Fraud Watch *PLUS* Clients (cardholder use): 1-866-842-5208

If you have other questions, please contact the TransFund Help Desk at 800-588-6816, option 3 during regular business hours or the Support numbers listed above after business hours and weekends.

TransFund®

1-800-588-6816 | transfund.com