Types of ATM Fraud

• Exchange of ATM Card / Card Theft
• Card Skimming
• Card Trapping / Cash Trapping
• VISHING
• ATM malware/ cash out attack/ jackpotting
• Keypad jamming
• Card Forking
The data skimmed can be transferred on to a computer system later.

**Information skimmed:-**

- name,
- credit / debit card number,
- expiry date, etc.,

It is used to create cloned credit / debit card.
Withdraw cash from ATM using a phone... how do they do it?

1. Install PLOUTUS TROJAN and phone inside ATM
2. Send SMS command to ATM
3. Collect the cash

Modus Operandi

The fraudster can open ATM's outer case with a sophisticated key

A pen drive carrying malware or a USB chord connected to a laptop is connected to the machine

Old machines with outdated software become prone to malware attacks

Once the malware infects the ATM, it can be controlled virtually

ATMs can be instructed to dispense cash without a card swipe
Point of Sale (POS)
<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
<th>Debit</th>
<th>Credit</th>
<th>Balance</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.05.17</td>
<td>CASH Deposited at GCC</td>
<td>5000.00</td>
<td></td>
<td>116163.21Cr</td>
</tr>
<tr>
<td>25.06.17</td>
<td>INTEREST CREDIT</td>
<td></td>
<td>1170.00</td>
<td>117333.21Cr</td>
</tr>
<tr>
<td>16.08.17</td>
<td>CASH Deposited at GCC</td>
<td>10000.00</td>
<td></td>
<td>127333.21Cr</td>
</tr>
<tr>
<td>24.09.17</td>
<td>OTHPG 014110 PAY+bills</td>
<td></td>
<td>5999.00</td>
<td></td>
</tr>
<tr>
<td>24.09.17</td>
<td>OTHPG 016997 PAY+bills</td>
<td></td>
<td>9999.00</td>
<td></td>
</tr>
<tr>
<td>24.09.17</td>
<td>SBIPG 0300153332870a Money - Zipcash</td>
<td>9999.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>24.09.17</td>
<td>SBIPG 030015335730a Money - Zipcash</td>
<td>5000.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>24.09.17</td>
<td>OTHPG 201318 PAY+bills</td>
<td></td>
<td>4999.00</td>
<td></td>
</tr>
<tr>
<td>24.09.17</td>
<td>SBIPG 0400212208150a Money - Zipcash</td>
<td>9998.00</td>
<td></td>
<td>32438.21Cr</td>
</tr>
<tr>
<td>24.09.17</td>
<td>SBIPG 0300153940510a Money - Zipcash</td>
<td>5000.00</td>
<td></td>
<td>27438.21Cr</td>
</tr>
<tr>
<td>24.09.17</td>
<td>OTHPG 203917 CUBBANKW</td>
<td>4998.00</td>
<td></td>
<td>22440.21Cr</td>
</tr>
<tr>
<td>24.09.17</td>
<td>SBIPG JU5682927782SBIBuddy</td>
<td>5000.00</td>
<td></td>
<td>17440.21Cr</td>
</tr>
<tr>
<td>25.09.17</td>
<td>OTHPG 047752 CUBBANKW</td>
<td>4998.00</td>
<td></td>
<td>12442.21Cr</td>
</tr>
<tr>
<td>25.09.17</td>
<td>OTHPG 056463 IDEAMONEY</td>
<td>4986.00</td>
<td></td>
<td>7456.21Cr</td>
</tr>
<tr>
<td>25.09.17</td>
<td>OTHPG 057447 IDEAMONEY</td>
<td>4987.00</td>
<td></td>
<td>2469.21Cr</td>
</tr>
<tr>
<td>25.09.17</td>
<td>OTHPG 059544 MPESA</td>
<td>1986.00</td>
<td></td>
<td>483.21Cr</td>
</tr>
</tbody>
</table>

Uncl Bal: 0.00  Clr Bal: 483.21 Cr;+MOD BAL: 0.00
<table>
<thead>
<tr>
<th>Date</th>
<th>Item Description</th>
<th>Quantity</th>
<th>Unit Price</th>
<th>Total Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>25.10.17</td>
<td>SBIPG K5632528568FLIPKART</td>
<td>14</td>
<td>1799.00</td>
<td>25186.00</td>
</tr>
<tr>
<td>25.10.17</td>
<td>SBIPG K56325285693FLIPKART</td>
<td>14</td>
<td>1799.00</td>
<td>25186.00</td>
</tr>
<tr>
<td>25.10.17</td>
<td>SBIPG K56325285603FLIPKART</td>
<td>14</td>
<td>1799.00</td>
<td>25186.00</td>
</tr>
<tr>
<td>25.10.17</td>
<td>SBIPG K56325285607FLIPKART</td>
<td>14</td>
<td>1799.00</td>
<td>25186.00</td>
</tr>
<tr>
<td>25.10.17</td>
<td>SBIPG K56325285613FLIPKART</td>
<td>14</td>
<td>1799.00</td>
<td>25186.00</td>
</tr>
<tr>
<td>25.10.17</td>
<td>SBIPG K56325285634FLIPKART</td>
<td>14</td>
<td>1799.00</td>
<td>25186.00</td>
</tr>
<tr>
<td>25.10.17</td>
<td>SBIPG K56325285639FLIPKART</td>
<td>14</td>
<td>1799.00</td>
<td>25186.00</td>
</tr>
<tr>
<td>25.10.17</td>
<td>SBIPG 01000316923353www.flipkart.com</td>
<td>14</td>
<td>1799.00</td>
<td>25186.00</td>
</tr>
<tr>
<td>25.10.17</td>
<td>SBIPG K56325285643FLIPKART</td>
<td>14</td>
<td>1799.00</td>
<td>25186.00</td>
</tr>
<tr>
<td>25.10.17</td>
<td>SBIPG K56325285666FLIPKART</td>
<td>14</td>
<td>1799.00</td>
<td>25186.00</td>
</tr>
<tr>
<td>25.10.17</td>
<td>SBIPG K56325285675FLIPKART</td>
<td>14</td>
<td>1799.00</td>
<td>25186.00</td>
</tr>
<tr>
<td>25.10.17</td>
<td>SBIPG K56325285685FLIPKART</td>
<td>14</td>
<td>1799.00</td>
<td>25186.00</td>
</tr>
<tr>
<td>25.10.17</td>
<td>SBIPG 0800000276699www.flipkart.com</td>
<td>14</td>
<td>1799.00</td>
<td>25186.00</td>
</tr>
<tr>
<td>25.10.17</td>
<td>SBIPG 0200021698197www.flipkart.com</td>
<td>14</td>
<td>1799.00</td>
<td>25186.00</td>
</tr>
<tr>
<td>25.10.17</td>
<td>SBIPG 0600000276295www.flipkart.com</td>
<td>14</td>
<td>1799.00</td>
<td>25186.00</td>
</tr>
</tbody>
</table>

Unc: Bal: 0.00  Cr: Bal: 476.22 Cr; MOD BAL: 0.00
Investigation of VISHING Fraud
Voice phishing / VISHING is typically used to steal Credit Card /ATM Card numbers, CVV Number, OTP or other Banking credential / information
Features of ATM Card

16 digits ATM Card Number

Expiry date of ATM Card

Card Holder’s name

CVV Number written at the back side of ATM Card
Your Signature Here  
(Very Important)

CVV Number  
(Always scratch this)
Track 1: Card number, holder name, expiration date

Track 2: Card number, expiration date

Track 3: Occasionally used by loyalty programs

Magnetic Strip

Signature Strip
Accused will ask for:

- ATM-cum-Debit card Number
- CVV number (Card Verification Value)
- One Time Password (OTP)
Accused will instruct to victim:

- To delete all the messages
- Not to inform anyone due to confidential nature of operation
Nature of transactions made by accused:

- Numbers of online transactions such as purchase of goods / electronic equipment's
- Online payments / Mobile / DTH recharge
- Transfer of fraudulent money:
  - To Wallet of the concerned Payment Gateway where accused had made fraudulent transactions
  - To Wallet of other Payment Gateway
  - To any other bank account
From the Complainant

Mobile Phone Number of the fraudster to be ascertained from the victim

Seizure of the following documents on production by the victim complainant:

- ATM-cum-Debit card in original
- Updated Savings Passbook
- SMS details received from the Bank about the online transactions made by the accused with date & time written in a paper by the complainant
- Mobile Phone Handset along with SIM Card (in which the SMSs were received) be seized and be left in zima
Step by step investigation procedure:

- **Letter to Bank:**
  - AOF (Account Opening Form) / Bank Account Statement of the complainant
  - Detailed particulars of each banking transaction
  - ATM-cum-Debit Card details of the complt.
  - Certificate u/s 2A of Bankers Book of Evidence Act, 1891
Letter to Mobile Service Provider:

- Subscriber Details
- Date of Activation
- CAF (Customer Acquisition / Application Form)
- CDR (Call Details Record) of the complainant as well as of the accused person for the relevant period
- Certificate u/s 65B (4) (c) of Indian Evidence Act, 1872
Online Payment Gateway
How Payment Gateways work:

Customer buys from an e-commerce site, makes payment by providing credit/debit/cash card details, or net banking related information.

The site passes on the details to a payment gateway company.

If it is a net banking transaction, payment gateway firm engages with the customers’ bank directly to collect the payment.
Letter to Online Payment Gateway:

- **Notice u/s 91 of Cr.P.C. to be issued**
- Detailed description of each fraudulent transaction with relevant to Wallet ID?
- **IP details of the computer system used along with date and time for committing the said fraudulent transaction?**
- Whether accused had created or registered any account in your website for committing the offence?
  - Date & time of registration / creation of ID
  - IP details along with date & time of the computer system used for registration/ creation of the account
  - Type of operating system of the computer system of the fraudster
  - Physical address of the computer system
- Mobile phone numbers / E-mail addresses of the accused used for registration or for generation of OTP or for any authentication process
- Mailing address of the accused
  - Whether accused had opened any wallet in your website for committing fraudulent transactions?
  - Date and time of creation of Wallet
  - IP details of the computer system used by the accused for creation of the said wallet?
  - What was the transaction limit set by the accused for the said Wallet?
  - Whether the said Wallet created by the accused was linked to any bank account?
  - Details of the bank account along with the bank name and IFSC Code may please be furnished.
  - Detailed transactions made by the accused through the said Wallet may please be furnished.
• Whether accused had purchased or made online shopping of any goods or articles through your website?

• **Counter foil receipt in respect of delivery of goods by online shopping website to the fraudster [DRS:- Delivery Run Sheet]**

• **Detailed particulars of Courier Agency or company personnel** along with his contact number or e-mail ID; who had delivered the purchased goods / products to the fraudster

• Date and time of delivery of goods

• Address of delivery of goods

• As these are fraudulent transactions, it is hence requested to kindly initiate the process for revert back of the defrauded amount to the bank account of the complainant.

• Certificate u/s 65B (4) (c ) of Indian Evidence Act, 1872
Letter to E-mail Service Provider:

- **Notice u/s 91 of Cr.P.C. to be issued**
- Account Registration Details of the e-mail account
- Log Details
- Mobile Phone Number used at the time of registration and updation of the e-mail account {registered mobile phone number}
- Secondary e-mail account
- Certificate u/s 65B (4) (c) of Indian Evidence Act, 1872
Letter to Internet Service Provider:

- End user details of IP Addresses
- CAF / NTC in respect of the user subscriber in respect of the alleged IP address
- Other relevant information in respect of the user subscriber that is the address of correspondence, contact number, e-mail IDs and billing details
- MAC ID of the alleged computer system / IMEI address of the computer resources with respect of the relevant IP address.
- Certificate u/s 65B of Indian Evidence Act, 1872
Letter to Bank:

• Detailed information as regards of the account holder in respect of the bank account of the accused:-
  • Name of the account holder
  • Correspondence address of the account holder
  • Contact number
  • Registered Mobile Number
  • E-mail account if any
  • Date of opening of bank account

• Original Account Opening Form \{AOF\} in respect of the aforesaid bank account.
• Original documents submitted by the account holder at the time of opening of the account, in compliance to the provisions of KYC norm.

• Account statement in respect of the aforementioned bank account for the period from ________________.

• Present status of the aforementioned bank account

• Whether ATM-cum-Debit card has been issued to the Customer by the Bank?

  • Card Number
  • Date of submission of application by the accused for issuing of ATM-cum-Debit card
  • Date of issue
  • Place of issue {on which address ATM Card was delivered to the customer}
  • Application submitted by the accused in the bank to provide ATM-cum-Debit card
• **To freeze the operation of the bank account.**

• On which date the said bank account has been frozen.

• Amount frozen may please be furnished.

• Whether the said bank account of the accused is being involved in any of the offence? If involved, kindly furnish the documents pertaining to the said aspect and the action taken by your bank into the said matter.

• Certificate u/s 2A of Bankers Book Evidence Act, 1891 may kindly be furnished along with the report.
Sample Reports
6. As processors, we therefore receive only limited information from the billing company and the banks. We maintain the electronic trail of such transactions which would typically have information on the IP address from which the transaction was initiated, date & time when the transaction was initiated, the billing company to whom the monies are to be paid, the mobile number (in case the billing company is a mobile service provider), and the payment amount for the transaction.

7. In respect of the transactions detailed in your aforementioned letter/mail, we have produced below, the details as available with us:

<table>
<thead>
<tr>
<th>Sr. No</th>
<th>Merchant Name</th>
<th>Transaction ID on our platform</th>
<th>E-wallet Number for which payment was made</th>
<th>Transaction Date and Time (IST)</th>
<th>Transaction Amount (Rs.)</th>
<th>IP Address from where transaction initiated</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IDEAMONEY</td>
<td>HHIMP5111166 9324</td>
<td>9934911 536</td>
<td>11/2/2017 17:59</td>
<td>4999</td>
<td>223.176.90 .125</td>
<td>SUCCESS</td>
</tr>
</tbody>
</table>

8. We request you to approach the above-mentioned merchants at following e-mail IDs for further assistance in the noted matter.

<table>
<thead>
<tr>
<th>Merchant</th>
<th>E-mail ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idea Money</td>
<td><a href="mailto:idea.moneycare@idea.adityabirla.com">idea.moneycare@idea.adityabirla.com</a></td>
</tr>
</tbody>
</table>

Please let us know in case you require any further information in this regard. We will be glad to render whatever assistance possible.
<table>
<thead>
<tr>
<th>First Name</th>
<th>Last Name</th>
<th>Date of birth</th>
<th>Mother Name</th>
<th>Date of wallet registration</th>
</tr>
</thead>
<tbody>
<tr>
<td>puja</td>
<td>kumari</td>
<td>21-Jun-97</td>
<td>mamta</td>
<td>21-Jun-16</td>
</tr>
</tbody>
</table>

5934011536
<table>
<thead>
<tr>
<th>Transaction Date and Time</th>
<th>Transaction Id</th>
<th>Service</th>
<th>From Entity</th>
<th>To Entity / Bank transfer</th>
<th>IFSC code</th>
<th>Amount (Rs)</th>
<th>Final Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>11-02-2017 18:02:45</td>
<td>11021710109713</td>
<td>Cash In online - Debit Card Idea</td>
<td>Customer 9934911536</td>
<td>32507010018644</td>
<td>UCBA0003257</td>
<td>4,999.00</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>12-02-2017 10:39:19</td>
<td>12021710236288</td>
<td>P2B-IMPS</td>
<td>Customer 9934911536</td>
<td>UCBA0003257</td>
<td>5,000.00</td>
<td>SUCCESS</td>
<td></td>
</tr>
</tbody>
</table>
Thank you ...