Procedure of Investigation of ATM Fraud / Credit Card Fraud

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


Camera
Card Skimmer
Keyboard Overlay


Receipt

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.


BBVA


KARTE
1 2 3
4 5 6
7 8 9
0


Skimmer for Data capture


Camera for PIN Capture
Skimmer for Data capture


False Front


REFER A FRIEND.
IT ADDS UP TO
$25 FOR BOTH
OF YOU.
Ask How.
camera underneath
skimmer


ATM
SCAMMERS


dgmali.en.alibaba.com


© FICO

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Old machines with outdated software become prone to malware attacks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


200

Point of Sale (POS)

Manmohan.pdf - Adobe Reader

File Edit View Window Help

Open | 2 / 2 | 143% | Tools | Fill & Sign | Comment

06.05.17	WITHDRAWAL TRANSFER BY CHEQUE				
	TRANSFER TO 035401324556			5000.00	116163.21Cr
10.05.17	CASH Deposited at GCC				
Uncl Bal: 0.00		Clr Bal: 116163.21 Cr:+MOD BAL: 0.00			
25.06.17	INTEREST CREDIT			1170.00	117333.21Cr
16.08.17	CASH Deposited at GCC			10000.00	127333.21Cr
Uncl Bal: 0.00		Clr Bal: 127333.21 Cr:+MOD BAL: 0.00			
24.09.17	OTHPG 014110	PAY*WWW OLACABS COM	9999.00		117334.21Cr
24.09.17	OTHPG 016997	PAY*WWW OLACABS COM	9999.00		107335.21Cr
24.09.17	SBIPG 030015353287	Ola Money - Zipcash	9999.00		97336.21Cr
24.09.17	SBIPG 030015353573	Ola Money - Zipcash	5000.00		92336.21Cr
24.09.17	OTHPG 201318	PAY*WWW FUTUREPAY CO I	49900.00		[illegible]
24.09.17	SBIPG 040021220815	Ola Money - Zipcash	9998.00		32438.21Cr
24.09.17	SBIPG 030015394051	Ola Money - Zipcash	5000.00		27438.21Cr
24.09.17	OTHPG 203917	CUBBANKW	4998.00		22440.21Cr
24.09.17	SBIPG JU5682927782	SBIBUDDY	5000.00		17440.21Cr
25.09.17	OTHPG 047752	CUBBANKW	4998.00		12442.21Cr
25.09.17	OTHPG 056468	IDEAMONEY	4986.00		7456.21Cr
25.09.17	OTHPG 057447	IDEAMONEY	4987.00		2469.21Cr
25.09.17	OTHPG 059544	MPESA	1986.00		483.21Cr
Uncl Bal: 0.00		Clr Bal: 483.21 Cr;+MOD BAL: 0.00			

25.10.17	SBIPG KS5632528582FLIPKART	1799.00	29390.22Cr
25.10.17	SBIPG KS5632528593FLIPKART	1799.00	27591.22Cr
25.10.17	SBIPG KS5632528603FLIPKART	1799.00	25792.22Cr
25.10.17	SBIPG KS5632528607FLIPKART	1799.00	23993.22Cr
25.10.17	SBIPG KS5632528613FLIPKART	1799.00	22194.22Cr
25.10.17	SBIPG 080000276641www.flipkart.com	1799.00	20395.22Cr
25.10.17	SBIPG KS5632528634FLIPKART	1799.00	18596.22Cr
		1799.00	16797.22Cr
25.10.17	SBIPG KS5632528639FLIPKART	1799.00	14998.22Cr
25.10.17	SBIPG 010031692335www.flipkart.com	1799.00	13199.22Cr
25.10.17	SBIPG KS5632528643FLIPKART	1799.00	11400.22Cr
25.10.17	SBIPG KS5632528666FLIPKART	1899.00	9501.22Cr
25.10.17	SBIPG KS5632528675FLIPKART	1899.00	7602.22Cr
25.10.17	SBIPG KS5632528679FLIPKART	1899.00	5703.22Cr
25.10.17	SBIPG KS5632528685FLIPKART	1849.00	3854.22Cr
25.10.17	SBIPG 080000276659www.flipkart.com	1849.00	2005.22Cr
25.10.17	SBIPG 020031698519www.flipkart.com	999.00	1006.22Cr
25.10.17	SBIPG 060000276295www.flipkart.com	530.00	476.22Cr

Uncl Bal: 0.00 Clr 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

ATM MACHINE

ATM Display Screen

Card Reader

ATM Keypad

Cash Dispenser

Maestro Card

Master Card

Features of ATM Card

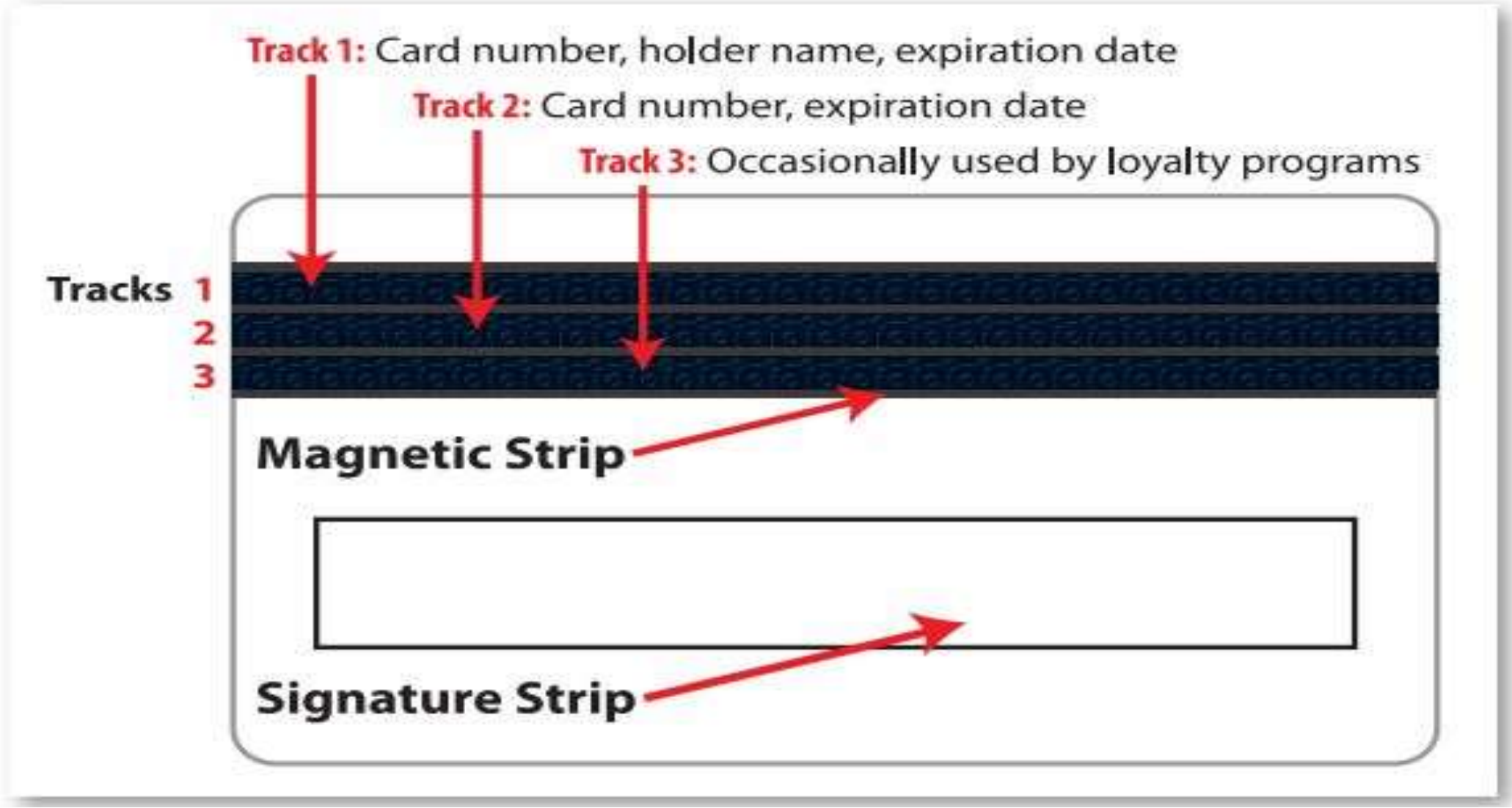
16 digits ATM Card Number

Expiry date of ATM Card

Card Holder's name

CVV Number written at the back side of ATM Card


Lee M. Cardholder
9999
123
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
Tracks 1
2
3
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:-

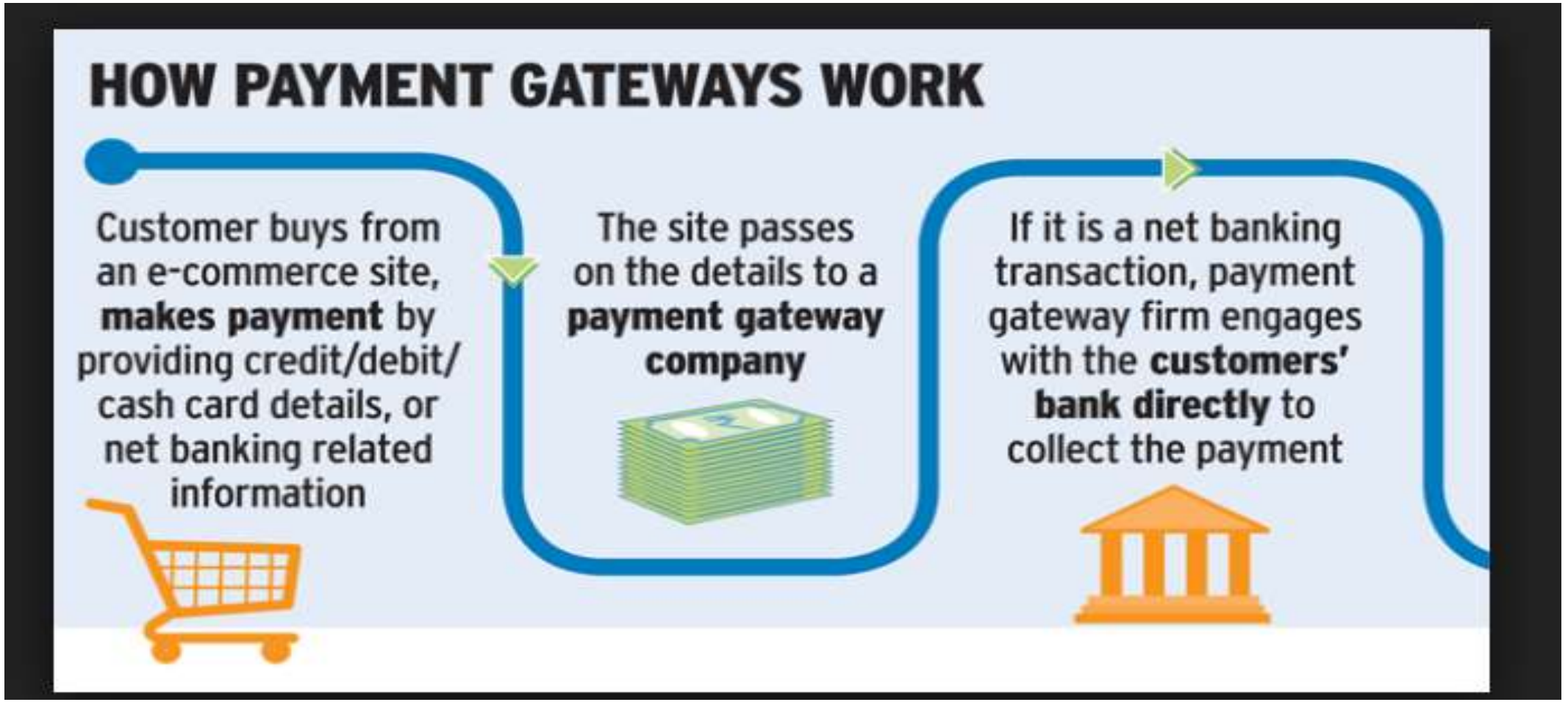
- **Letter to Bank:**
  - AOF (Account Opening Form) / Bank Account Statement of the complainant
  - Detailed particulars of each banking transaction
  - ATM-cum-Debit Card details of the complt.
  - Certificate u/s 2A of Bankers Book of Evidence Act, 1891

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:



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.

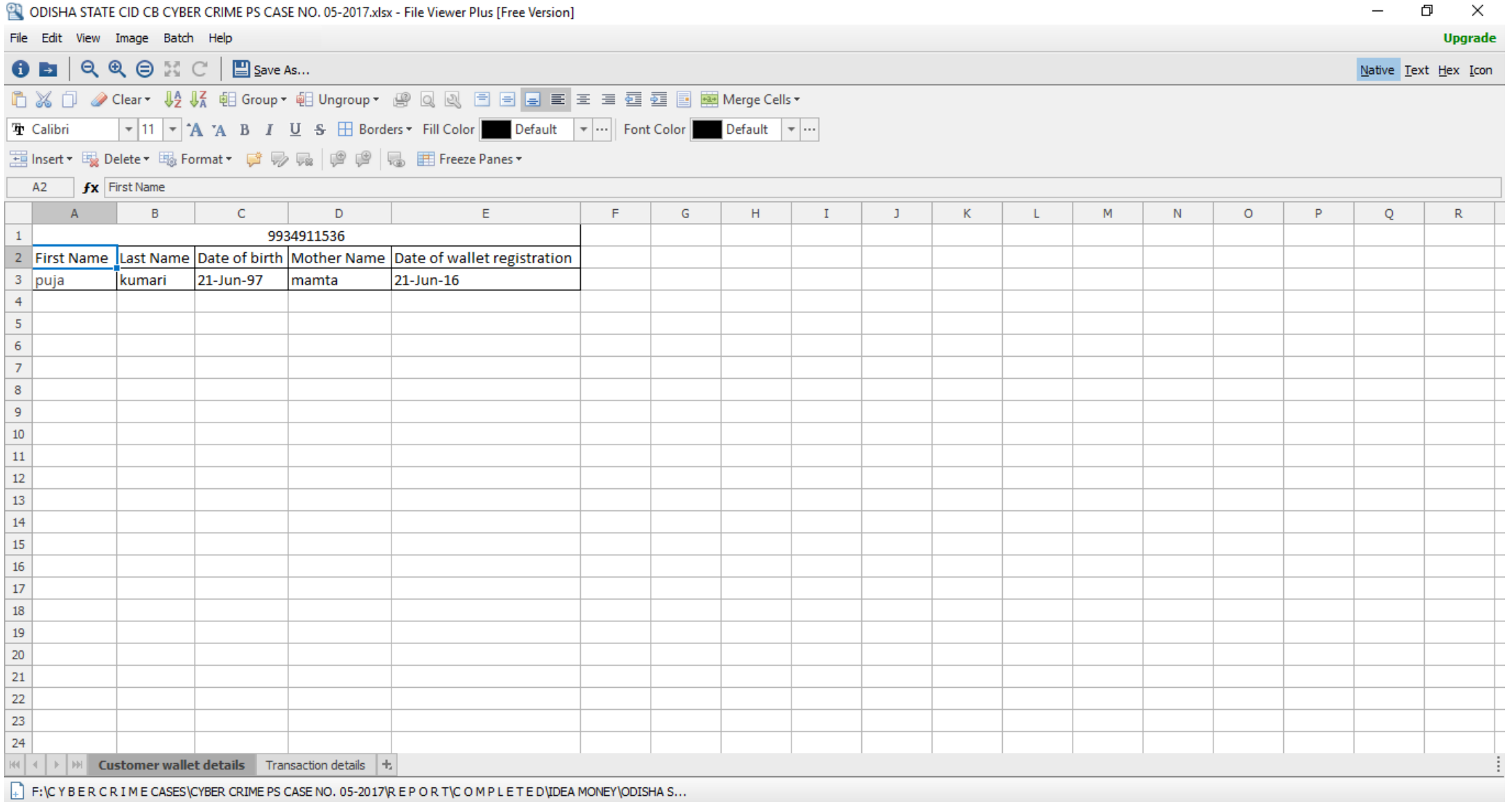
7. In respect of the transactions detailed in your aforementioned letter/mail, we have produced below, the details as available with us:

Sr. No	Merchant Name	Transaction ID on our (Indiadeas.com) platform	E-wallet Number for which the payment was made	Transaction Date and Time (IST)	Transaction Amount (Rs.)	IP Address from where transaction initiated	Status
1	IDEAMONEY	HHMP5111669324	9934911536	11/2/2017 17:59	4999	223.176.90.125	SUCCESS

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

Merchant	**E-mail ID**
Idea Money	ideamoneycare@idea.adityabirla.com

Please let us know in case you require any further information in this regard. We will be glad to render whatever assistance possible.


ODISHA STATE CID CB CYBER CRIME PS CASE NO. 05-2017.xlsx - File Viewer Plus [Free Version]
File Edit View Image Batch Help
Upgrade
Save As...
Native Text Hex Icon
Clear Group Ungroup Merge Cells
Calibri 11 Borders Fill Color Default Font Color Default
Insert Delete Format Freeze Panes
A2 First Name
9934911536
First Name Last Name Date of birth Mother Name Date of wallet registration
puja kumari 21-Jun-97 mamta 21-Jun-16
Customer wallet details Transaction details
F:\C Y B E R C R I M E CASES\CYBER CRIME PS CASE NO. 05-2017\R E P O R T\C O M P L E T E D\IDEA MONEY\ODISHA S...

ODISHA STATE CID CB CYBER CRIME PS CASE NO. 05-2017.xlsx - File Viewer Plus [Free Version]

File Edit View Image Batch Help Upgrade

Save As... Native Text Hex Icon

Clear Group Ungroup Merge Cells

Arial 11 Borders Fill Color 0.113.188 Font Color White

Insert Delete Format Freeze Panes

A1 Transaction Date and Time

	A	B	C	D	E	F	G	H	I	J	K
1	Transaction Date and Time	Transaction Id	Service	From Entity	To Entity / Bank transfer	IFSC code	Amount (Rs)	Final Status			
2	11-02-2017 18:02:45	11021710109713	Cash In online - Debit Card	Idea	Customer 9934911536		4,999.00	SUCCESS			
3	12-02-2017 10:39:19	12021710236288	P2B-IMPS	Customer 9934911536	32570110018644	UCBA0003257	5,000.00	SUCCESS			
4								SUCCESS			
5											
6											
7											
8											
9											
10											
11											
12											
13											
14											
15											
16											
17											
18											
19											
20											
21											
22											
23											

Customer wallet details | Transaction details

F:\CYBER CRIME CASES\CYBER CRIME PS CASE NO. 05-2017\REPORT\COMPLETED\IDEA MONEY\ODISHA S...


Thank you ...