APPENDIX
APPENDIX – I
PAYMENT GATEWAYS

1. Anacom, Anacom Merchant Services, United States
2. Authorize.net, Authorize.net, United States
3. Banco Comercial Portugues, Banco Comercial Português, Portugal
4. Bank Merchant POS (BMP), Bank of China, China
5. Beanstream, Beanstream Internet Commerce, Inc., Canada
6. Bibit, Bibit Internet Payments, Netherlands
7. Bill4me.com, Facilitate I.T. Inc., Canada
8. Biz*Star PX, Shanghai Shared Data Network Co. Ltd (SSDN), Singapore
9. Business Gateway Service, WorldCom, Japan
10. Buy-Line, Bank of New Zealand, New Zealand
11. CAFIS, NTT Data Corp., Japan
12. Cambist, Cambist Merchant Solutions, United States
13. Camtech, Camtech Corp., Australia
14. CCNow, CCNow, Inc., United States
15. Chinatrust, Chinatrust Commercial Bank (CTCB), Taiwan, Province of China
16. CIBC, Canadian Imperial Bank of Commerce, Canada
17. CIPAS Indonesia, PT. CIPAS Indonesia, Indonesia
18. iBill, Internet Billing Company, Ltd., United States
19. CitiBank
20. India, CitiBank India, India
22. ClickBank, Keynetics Inc., United States
23. ClickPay, Professo, LLC, United States
24. Ecgate, Ecnet, South Africa
25. CMB, China Merchants Bank, China
26. Comtrust, Comtrust, United Arab Emirates
27. CyberCash, VeriSign Payment Services, United States
28. CyberSource, CyberSource Corp., United States
29. DataCash, DataCash Ltd., United Kingdom
30. DirectLink, Plug 'n Pay Technologies, Inc., United States
31. DnB, DnB - Den norske Bank, Norway
32. E-Commerce Africa, E-Commerce Africa, Netherlands
33. ePDQ, Barclaycard Merchant Services, United Kingdom
34. E-Payment,
35. Interactive Worldwide Limited, Australia
36. e4Sure, e4asia Inc., Thailand
37. CyberMUT, Groupe Crédit Mutuel, France
38. EBS, Electronic Billing
39. Systems AG, Germany
40. ECHOnline, Electronic Clearing House, Inc.,
41. eops, eops AG, Germany
42. ePagos, ePagos Merchant Services, United States
43. eSec Payment Service, eSec Ltd., Australia
44. eStores, Bank of America, United States
45. EuroDebit, Moreband Corp. NV, Netherlands Antilles
46. FirstEcom, First Ecom, Hong Kong
47. GestPay, Banca Sella S.p.A., Italy
48. HDFC Bank, HDFC Bank, Ltd., India
49. I.N.G, Internet Networking Group, Netherlands
50. IntelliPay, IntelliPay Inc., United States
51. IPGS, Visa, United States
52. iVeri, eCompany Ltd., South Africa
53. JustGiving.com, Justgiving, United Kingdom
54. Ka-Chingg and TPG, iPayment Technologies, United States
55. Kagi, Kagi, United States
56. LinkPoint, CardService International, United States
57. LiveProcessor, Paymentplus, Inc., United States
58. MultiCards.com, De Postel BV, Netherlands
59. NetBanx, NetBanx Ltd., United Kingdom
60. Netbilling, Automated Billing Services, United States
61. Online Charge, Innuity, Inc., United States
63. Pago PAY, Pago eTransaction Services GmbH, Germany
64. PAY@db, Deutsche Bank, Germany
65. PayCash.ru, Alkor Group of Companies, Russian Federation
66. PayControl, Nettcetera AG, Switzerland
67. PayFlow, VeriSign Payment Services, United States
68. PaymentService, PaymentService.at, Austria
69. PayPal, PayPal, United States
70. PaySeal, ICICI ePayments Ltd., India
71. PayWare, Trintech Group plc, Ireland
72. PayWay, Nobil IT Corporation, Canada
73. PlanetPayment, Planet Group Inc., United States
74. QPAY and QTILL, QENTA paymentsolutions GmbH, Austria
75. QSI Client Class, QSI Payments, Australia
76. Secure-e-pay, Global Tele-Systems Ltd., India
77. SecurePay, SecurePay Pty Ltd., Australia
78. SecureTrading, SecureTrading, United Kingdom
79. Setcom, Setcom (Pty) Ltd., South Africa
80. SIPS, Siam Commercial Bank PCL., Thailand
81. Solo e-payment, Solo Market/Merita Bank Plc, Finland
82. Speedpay, E Commerce Group, United States
83. SurePay, SurePay LP, United States
84. Telecharge Canada, TeleCharge Canada, Canada
85. Telecommerce, France Telecom, France
86. Thirt, Thirt.com, South Africa
87. TOPGate, Shanghai Bankcard Network Services Corp., China
88. USA ePay, GorCorp Inc., United States
89. VIP, Virbus AG, Germany
90. WebCollect, GlobalCollect, Netherlands
91. Webmoney.ru, WebMoney Transfer, Russian Federation
92. Webpay, Transbank, Chile
93. WorldPay, WorldPay plc, United Kingdom
APPENDIX – II


Year 2010

- Houston Computer Administrator Sentenced to 12 Months in Prison for Hacking Former Employer’s Computer Network (July 6, 2010)
- Dublin Woman Pleads Guilty to Hacking Email Accounts and Deleting Documents in Domestic Relations Dispute (July 2, 2010)
- Blaine Man Indicted for Hacking into Neighbor’s Wireless Internet System and Posing As the Neighbor to Email Child Pornography and Threats to the Vice President (June 24, 2010)
- Nantucket Man Arrested and Charged with Operating International Online "Phishing" Scheme to Steal Income Tax Refunds (June 24, 2010)
- O’Fallon Man Indicted for Internet Fraud in Connection with 2006 St. Louis Cardinal Playoff Tickets Scheme (June 24, 2010)
- Orange County Man Suspected of Hacking Computers Arrested on Federal Charges Related to Demands For Sexually Explicit Videos from Women and Teenage Girls (June 22, 2010)
- Another Pleads Guilty in Botnet Hacking Conspiracy (June 10, 2010)
- U.S. Indicts Ohio Man and Two Foreign Residents in Alleged Ukraine-Based "Scareware" Fraud Scheme That Caused $100 Million in Losses to Internet Victims Worldwide (May 27, 2010)
- Student Convicted with Using University Computer Network for Denial of Service Attacks and to Control Other Computers (via "Botnet" Zombies) (May 26, 2010)
- Arlington Security Guard, Who Hacked into Hospital’s Computer System, Pleads Guilty to Federal Charges (May 14, 2010)
- Chico Man Pleads Guilty to Embezzling $693,000 from Charity (May 14, 2010)
Las Vegas Man Pleads Guilty to Creating and Selling Cookie-Stuffing Program (May 14, 2010)

Student Charged with Using University Computer Network for Denial of Service Attacks and to Control Other Computers (via "Botnet" Zombies) (May 14, 2010)

Grand Jury Returns Indictment Charging Nine Individuals with Exceeding Authorized Computer Access (May 12, 2010)

Indian National Sentenced to 81 Months in Prison for Role in International Online Brokerage "Hack, Pump and Dump" Scheme (April 26, 2010)

‘Hacker’ Indicted in Massive Tax, Mail, and Wire Fraud Scheme (April 8, 2010)

Computer Hacker Sentenced to 37 Months in Prison in Manhattan Federal Court for Scheme to Steal and Launder Money from Brokerage Accounts (April 7, 2010)

Louisville Man Charged in Computer Fraud Scheme (April 7, 2010)

Leader of Hacking Ring Sentenced for Massive Identity Thefts from Payment Processor and U.S. Retail Networks (March 26, 2010)

Illinois Man Sentenced to Two and a Half Years in Prison for Posting Nude Videos of ESPN Reporter on Internet (March 15, 2010)

Manhattan U.S. Attorney Charges California Man with Cyber-Extortion of New York-Based Insurance Company (March 8, 2010)

Four Indicted in $25 Million Scheme Defrauding and Hacking Ticketmaster, Tickets.com, and Other Ticket Vendors (March 1, 2010)

Harris County Deputy Sheriff Indicted for Disclosing Confidential Information for Cash (February 24, 2010)

"Iceman" Computer Hacker Receives 13-year Prison Sentence (February 12, 2010)

• Las Vegas Man Charged with Creating and Selling Cookie-stuffing Program (February 9, 2010)
• Kingdom of Sweden Accepts Request for Transfer of Prosecution in Case Involving Swedish National Charged with Hacking and Trade Secret Theft (February 8, 2010)
• Resident of India Pleads Guilty in International Online Brokerage "Hack, Pump and Dump" Scheme (February 5, 2010)
• Hacker Pleads Guilty to Infiltrating VOIP Networks and Reselling Service for Profit (February 3, 2010)
• Nebraska Man Agrees to Plead Guilty in Attack of Scientology Websites Orchestrated by 'anonymous' (January 25, 2010)
• Former Standard Mortgage Corporation Clerk Sentenced to 30 Months in Federal Prison for $1 Million Computer Fraud (January 14, 2010)
• Romanian Citizen Pleads Guilty to Federal Spamming Charge (January 14, 2010)
• Ninety-month Sentence for Man Who Emailed Threats to a Columbus Company, Florida Legislator (January 7, 2010)

Year 2009
• Major International Hacker Pleads Guilty for Massive Attack on U.S. Retail and Banking Networks (December 29, 2009)
• Hacker Sentenced for Providing Data Theft Tool in National Identity Theft Case (December 23, 2009)
• Former Inmate Sentenced for Hacking Prison Computer (December 22, 2009)
• Charges Filed in P2P Scheme to Access Bank Accounts and Transfer Fund (December 8, 2009)
• Six Individuals Sentenced for Multi-Million Dollar E-Mail Stock Fraud Scheme (November 24, 2009)
• Detroit Spammer and Three Co-Conspirators Sentenced for Multi-Million Dollar E-Mail Stock Fraud Scheme (November 23, 2009)
• Indictment Filed In Comcast Website Redirection Case (November 19, 2009)
• Last Defendant Sentenced in Swatting Conspiracy (November 16, 2009)
• Alleged International Hacking Ring Caught in $9 Million Fraud: Major Credit Card Processor Victimized in Elaborate Theft of Account Numbers (November 10, 2009)
• Two Men Charged with Computer Intrusion (November 4, 2009)
• West Coast Man Charged with Developing and Distributing Cable Network Hacking Tools (November 2, 2009)
• Former CEO of Yousendit Charged with Denial of Service of Attack (October 29, 2009)
• Computer Hacker Fugitive Extradited for Cybercrimes Relating to VOIP Telephone Services (October 15, 2009)
• CBP Officer Charged with Unlawful Access to Government Databases (October 8, 2009)
• One Hundred Linked to International Computer Hacking Ring Charged by United States and Egypt in Operation Phish Phry (October 7, 2009)
• Former Dupont Chemist Charged (October 2, 2009)
• Plumas Lake Man Sentenced to One Year and Three Months in Prison for Computer Fraud (September 17, 2009)
• Former Inmate Pleads Guilty to Hacking Prison Computer (September 15, 2009)
• Former Standard Mortgage Corporation Clerk Pleads Guilty to Computer Fraud Involving over One Million Dollar Theft (September 15, 2009)
• International Hacker Pleads Guilty for Massive Hacks of U.S. Retail Networks (September 11, 2009)
• Charges Filed Involving Interception of Internet Email and Computer Keystrokes (September 10, 2009)
• Alleged International Hacker Indicted for Massive Attack on U.S. Retail and Banking Networks (August 17, 2009)
• Former Standard Mortgage Corporation Clerk Charged with Computer Fraud (August 12, 2009)
• Second Defendant in Internet Scheme That Defrauded Trucking Companies Sentenced to Federal Prison (August 10, 2009)
• Federal Grand Jury Indicts Arlington Security Guard for Hacking into Hospital’s Computer System (July 23, 2009)
• Houston Computer Administrator Sentenced to Two Years in Prison for Hacking Former Employer’s Computer Network (July 15, 2009)
• Miami Man Sentenced in Computer Fraud Offense (July 14, 2009)
• DMCA Conspiracy Indictment Filed Involving Efforts to Crack DISH Encryption System (July 13, 2009)
• Virginia Software Writer Pleads Guilty to Aiding and Abetting Detroit Spam Conspiracy (July 7, 2009)
• Arlington Security Guard Arrested on Federal Charges for Hacking into Hospital’s Computer System (June 30, 2009)
• FBI Arrests Man behind a Host of Website Attacks- Including Rollingstone.com (June 30, 2009)
• “Iceman,” Founder of Online Credit Card Theft Ring, Pleads Guilty to Wire Fraud Charges (June 29, 2009)
• Detroit Spammer and Four Co-Conspirators Plead Guilty to Multi-Million Dollar E-mail Stock Fraud Scheme (June 22, 2009)
• Houston Man Indicted for Trafficking Counterfeit Computer Products (June 12, 2009)
• International Telephone Hacking Conspiracy Busted; Indictment in the United States, Arrests and Searches in Italy, and Continued Operations in the Philippines (June 12, 2009)
• Ohio Man was Sentenced to 21 Months in Prison in Connection with Recent Conviction for Violation of the Telephone Records and Privacy Act of 2006 (June 3, 2009)
• New Jersey Man Pleads Guilty to Launching Attack That Shut down Church of Scientology Websites (May 11, 2009)
• Swedish National Charged with Hacking and Theft of Trade Secrets Related to Alleged Computer Intrusions at Nasa and Cisco (May 5, 2009)
• Computer Administrator Pleads Guilty to Hacking Former Employer’s Computer System (May 1, 2009)
• San Diego Man Arrested for Conspiracy to Defraud the United States Regarding Claims (April 30, 2009)
• Laid off Computer Systems Administrator at Financial Firm Admits Attempting to Extort Better Severance Terms (April 27, 2009)
• Virginia Man Pleads Guilty to Selling Counterfeit Computer Software Worth $1 Million (April 16, 2009)
• Florida Man Arrested on Federal Sex Trafficking Charges for Prostituting Girl He Solicited on Internet (April 15, 2009)
• Owner and Operator of Massachusetts Computer Parts Company Pleads Guilty to Wire Fraud and Money Laundering in Connection with $15.4 Million Dollar Cisco Networking Equipment Fraud (April 10, 2009)
• Maple Grove Man Sentenced for Wire Fraud, Identity Theft (March 31, 2009)
• Statement of Rita M. Glavin, Acting Assistant Attorney General, Criminal Division, Concerning "Do the Payment Card Industry Standards Reduce Cybercrime?" (March 31, 2009)
• Upland Man Indicted for Allegedly Damaging Computer Systems Used to Monitor Off-shore Oil Platforms (March 17, 2009)
• Information Security Consultant Sentenced to 4 Years in Prison in Federal Wiretapping and Identity Theft Case (March 4, 2009)
• Two Plead Guilty to Defrauding Trucking Companies in Multi-million Dollar Scheme That Used Internet Site (February 24, 2009)
• Three Charged in Movie Piracy Cases Involving Illegal Posting of Theatrical Films on Internet (February 20, 2009)
• Texas Man Sentenced to 41 Months in Prison for Selling Counterfeit Software Worth $1 Million on Web Sites (February 17, 2009)
• Harvey Man Sentenced for Criminal Infringement of Trademarks and Copyrighted Materials (February 5, 2009)
• Individual Pleads Guilty in Swatting Conspiracy Case (January 29, 2009)
• Manhattan U.S. Attorney Charges Operator of Massmodz.com for Selling Hacked Cable Modems (January 28, 2009)
• Ex-hostgator.com Employee Sentenced for Computer Intrusion (January 26, 2009)
• New York City Police Sergeant Pleads Guilty to Accessing and Disseminating Information from Terrorist Watch List (January 14, 2009)
• Blaine Man Pleads Guilty to Sabotaging Former Employer's Computer System (January 13, 2009)
• KC Man Pleads Guilty to Cyberstalking: False Web Site Ads Invited Strangers to Victim's Home for Sexual Encounters (January 7, 2009)

Year 2008
• First Indictment Filed Under Telephone "Pretexting" Statute (December 30, 2008)
• "Chinese Connection" Defendant Pleads Guilty in Ralsky Spam and Stock Fraud Conspiracy (December 16, 2008)
• Husband and Wife Plead Guilty to Large-scale Copyright Fraud with Large Forfeiture of Assets (December 4, 2008)
• Multi-million Dollar Home Equity Line of Credit, Identity Theft and Computer Intrusion Ring Busted (November 24, 2008)
• Three Plead Guilty to Bank-Fraud Conspiracy (November 20, 2008)
• Juvenile Computer Hacker Pleads Guilty (November 18, 2008)
• Former Massachusetts Inmate Arrested for Hacking Prison Computer to Access Prison Management Program (November 6, 2008)
• Former IT Manager Sentenced to Prison for Hacking into Previous Employer’s Computer System and Causing Damage (November 3, 2008)
• San Jose Woman Charged with Fraud in Connection with a Protected Computer (October 30, 2008)
• Hacker Charged with Providing Data Theft Tool in National Identity Theft Case (October 29, 2008)
• New Jersey Man Charged with Attacking Church Of Scientology Websites in the Name of ‘Anonymous’ (October 17, 2008)
• Second Guilty Plea Entered in Ralsky Spam Conspiracy (October 17, 2008)
• Seven Members of Romanian Organized Crime Group Indicted in International Wire Fraud Scheme (October 16, 2008)
• Lansing Spammer Pleads Guilty (October 14, 2008)
• Vice President of Sales of Minnesota Computer Equipment Company Pleads Guilty to Scheme to Defraud Cisco of Computer Networking Equipment: Faris Fraudulently Conspired to Obtain over $400,000 in Equipment From Cisco Under the SMARTnet Service Contract Program (October 10, 2008)
• Former Connecticut State Trooper Pleads Guilty to Improperly Accessing a Government Computer (October 9, 2008)
• Tennessee Man Indicted for Alleged Hack of Governor Sarah Palin’s E-Mail Account (October 8, 2008)
• Computer Hacker Sentenced to Two Years in Federal Prison (October 7, 2008)
• Romanian National Pleads Guilty to Possessing Unauthorized Credit Cards Numbers, Identity Theft (October 7, 2008)
• San Diego Man Arraigned on Intentionally Damaging Computers Charge after Accessing Former Employer's Network and Defacing Web Page (October 7, 2008)
• San Diego Area Teacher Arraigned on Computer Hacking Charges for Gaining Unauthorized Access to E-mail Accounts of School Employees and for Reading Their Email (October 6, 2008)
- Two European Men Charged with Conspiring to Launch Cyberattacks against Websites of Two U.S. Companies (October 2, 2008)
- Auburn Man Indicted for Online Extortion (October 1, 2008)
- Former Bridgeport Tax Preparer Pleads Guilty to Filing False Claims for Tax Refunds and Computer Fraud (September 25, 2008)
- Man Charged with Intentionally Causing Damage to a Protected Computer and Four Counts of Extortion (September 22, 2008)
- TJX Data Theft Conspirator Pleads Guilty (September 22, 2008)
- PSU-Harrisburg Student Sentenced after Making Threats on Myspace (September 18, 2008)
- Washington State Woman Sentenced to 13 Months' Imprisonment for Role in Theft of Funds (September 11, 2008)
- Federal Jury Convicts Shreveport Stockbroker for Internet Threats (September 10, 2008)
- West Haven Man Involved in Email Phishing and Spamming Scheme Sentenced to Two Years in Prison (September 10, 2008)
- Malaysia Resident Sentenced to Two Years in Prison for Role in International Online Brokerage Scheme (September 8, 2008)
- Computer Tech Pleads Guilty to Identity Theft of Calpine Corporation Executive (September 2, 2008)
- Sacramento Man Sentenced for Using the Internet to Send Threatening Emails (August 29, 2008)
- Des Moines Man Indicted for Internet Threats of Violence and Identity Theft: Man Made Multiple Threats to Boeing Company and Anacortes Oil Refinery (August 28, 2008)
- Greenville Man Sentenced to Prison for Computer Hacking (August 28, 2008)
- Prison Terms Imposed In Access Device Fraud Case (August 28, 2008)
- Man Admits Six Flags Computer Sabotage (August 26, 2008)
- Former Television News Anchor Pleads Guilty to Computer Crime (August 22, 2008)
• Brazilian Man Charged in Conspiracy to Infect More Than 100,000 Computers Worldwide with Malicious Software (August 21, 2008)
• KC Man Pleads Guilty to Identity Theft, Credit Card Fraud (August 19, 2008)
• Mastermind of Elaborate Internet "Phishing" Scheme Sentenced to Seven Years in Federal Prison (August 14, 2008)
• Fact Sheet: Department of Justice Efforts to Combat Cyber Crimes (August 5, 2008)
• Retail Hacking Ring Charged for Stealing and Distributing Credit and Debit Card Numbers from Major U.S. Retailers: More Than 40 Million Credit and Debit Card Numbers Stolen (August 5, 2008)
• Romanian Citizen Admits Role in International Phishing Scheme (July 22, 2008)
• Digital Currency Business E-gold Pleads Guilty to Money Laundering and Illegal Money Transmitting Charges (July 21, 2008)
• Former Television News Anchor Charged with Computer Crime (July 21, 2008)
• Brooklyn Man Sentenced to 30 Months in Prison in Massive AOL Spam Scheme (July 15, 2008)
• Charges for "Trading with the Enemy" and Unauthorized Access to a Protected Computer (July 15, 2008)
• Largo Man Sentenced for Stealing Consumer Information (July 10, 2008)
• Former City of Newark Technology Contractor Admits Defrauding Cisco Systems of Millions of Dollars (July 2, 2008)
• Four Defendants Sentenced on Aggravated Identity Theft and Computer Fraud Charges (June 30, 2008)
• Individuals Named in Swatting Conspiracy Charged with Obstruction of Justice (June 27, 2008)
• Maple Grove Man Pleads Guilty to Wire Fraud, Identity Theft (June 27, 2008)
• Wyoming Man Charged with Infecting Thousands of Computers with 'Trojan' that He Used to Commit Fraud (June 27, 2008)
• Former Employee Indicted for Intentional Damage to Webhosting Data (June 26, 2008)
• Illinois Woman Pleads Guilty to Manufacturing Fake IDs (June 25, 2008)
• Houston Resident Indicted on Computer Hacking Charge (June 24, 2008)
• Man Arrested for Stealing Identities from Internet Gambling Site for Large Identity Theft Ring (June 23, 2008)
• Romanian National Returned to U.S. to Face Charges (June 13, 2008)
• New York Woman Sentenced to 46 Months in Prison for Internet Fraud Scheme (June 12, 2008)
• International Computer "Hacker" Sentenced to More Than Three Years in Federal Prison (June 11, 2008)
• Computer Hacker Pleads Guilty and Agrees to Two Years in Federal Prison (June 10, 2008)
• Ohio Resident Sentenced to 33 Months in Prison and Ordered to Pay Almost $2 Million in Restitution to Cisco Systems, Inc (June 10, 2008)
• California Man Sentenced to Over 5 Years' Imprisonment for Computer Hacking Conviction (June 9, 2008)
• Three Individuals Indicted by Federal Grand Jury with Conspiracy to Exceed Authorized Access of a Government Computer (June 5, 2008)
• Indictment in Baton Rouge, Louisiana, on Charges of Conspiracy, Wire Fraud, Mail Fraud, Money Laundering, Access Device Fraud, Aggravated Identity Theft, Bank Fraud, Computer Fraud, and Obstruction of Justice (June 3, 2008)
• Tucson Man Sentenced to over 5 Years in Prison for Aggravated Identity Theft (June 3, 2008)
• Plumas Lake Man Charged with Computer Fraud: Internet Scheme Used to Steal Micro-Deposits (May 28, 2008)
• Plumas Lake Man Charged with Computer Fraud (May 28, 2008)
• Man Pleads Guilty in Blast Fax Fraud Case (May 22, 2008)
• 38 Individuals in U.S. and Romania Charged in Two Related Cases of Computer Fraud involving International Organized Crime: International Law Enforcement Cooperation Leads to Disruption of Organized Crime Ring Operating in U.S. and Romania (May 19, 2008)
• Missouri Woman Indicted on Charges of Using Myspace to ‘Cyber-Bully’ 13-year-old Who Later Committed Suicide (May 15, 2008)
• Ringleaders in "Swatting/Spoofing" Conspiracy Sentenced (May 15, 2008)
• Hackers Indicted for Stealing Credit and Debit Card Numbers from National Restaurant Chain (May 12, 2008)
• KC Man Indicted for Cyberstalking (May 9, 2008)
• Military Computer Contractor Pleads to Unauthorized Access to Military Database and Id Theft (May 2, 2008)
• One of Colorado’s Largest Internet Spammers Sentenced to Federal Prison (April 28, 2008)
• Former Anniston Army Depot Employee Pleads Guilty to Computer Fraud and Theft (April 24, 2008)
• Nigerian Man Pleads Guilty and Is Sentenced to 18 Months by Nigerian Court for Computer Intrusion in the United States (April 22, 2008)
• Information Security Consultant Pleads Guilty to Federal Wiretapping and Identity Theft Charges (April 16, 2008)
• Foreign National Sentenced to Nine Years in Prison for Hotel Business Center Computer Fraud Scheme (April 11, 2008)
• Houston Man Pleads Guilty to Hacking Former Employer’s Computer System (April 9, 2008)
• St. Stephen Man Sentenced to 15 Years in Prison for Sexual Assault, Fraud, Witness Tampering and Extortion Scheme (April 7, 2008)
• Five Men Charged in Software Piracy Conspiracy (April 2, 2008)
• Former Information Technology Employee of Pentastar Aviation
  Sentenced for Computer Intrusion and Destroying Payroll and
  Personnel Records (March 20, 2008)
• West Haven Man Involved in Email Phishing and Spamming
  Scheme Pleads Guilty (March 18, 2008)
• Seattle Man Sentenced to 51 Months in Prison for ID Theft Scheme
  That Used Computer File Sharing Programs: First Conviction in the
  Country Involving Peer to Peer File Sharing Programs (March 17,
  2008)
• Seattle Spammer Pleads Guilty to Mail Fraud, Spam and Tax
  Charges: Man Sold Spamming Software and Spamming Services
  Impacting Millions of Computers (March 14, 2008)
• International Computer “Hacker” Convicted in Federal Court (March
  6, 2008)
• KC Man Sentenced for Computer Hacking (March 4, 2008)
• Indonesian Sentenced to 10 Months in Prison for Hacking into Hotel
  Business Kiosks and Stealing Credit Card Data (March 3, 2008)
• David U. Haltinner Sentenced to 50 Months of Imprisonment for
  Selling Approximately 637,000 Stolen Credit Card Numbers
  (February 26, 2008)
• Chinese Chemist Indicted for Theft of Trade Secrets (February 21,
  2008)
• IRS Employee Pleads Guilty to Charge of Unauthorized Access to a
  Government Computer (February 14, 2008)
• Bakersfield Law Student Sentenced in Email Harassment Scheme
  (February 13, 2008)
• Ohio Man charged in scheme to obtain $1.9 million in equipment
  from Cisco under SMARTnet Service Contract Program (February
  11, 2008)
• Young ‘Botherder’ Pleads Guilty to Infecting Military Computers and
  Fraudulently Installing Adware (February 11, 2008)
• Fairfax County Police Sergeant Pleads Guilty to Unauthorized
  Computer Access (January 31, 2008)
• KC Woman, Man Indicted for Computer Crime, Identity Theft (January 16, 2008)
• Five Years in Prison for Takeover of Online Bank Account (January 14, 2008)
• Evansville Man Sentenced to Prison for Computer Intrusion (January 10, 2008)
• Former St. Cloud Hospital Employee Pleads Guilty to Planting "Logic Bomb" on Hospital Computer (January 10, 2008)
• Norcross Man Sentenced for Hacking Cox Communications’ Computer and Telecommunications System: Former Employee’s Intrusion Shut Down Services in Texas, Las Vegas, New Orleans, and Baton Rouge (January 10, 2008)
• Foreign National Pleads Guilty in Complex Computer Fraud Scheme Victimizing Hundreds of Individuals (January 9, 2008)
• Four Minnesota Residents Charged in California with Scheme to Defraud Cisco of Computer Networking Equipment: Defendant Fraudulently Conspired to Obtain over $400,000 in Equipment From Cisco under the SMARTnet Service Contract Program (January 9, 2008)
• Former Systems Administrator Gets 30 Months in Prison for Planting "Logic Bomb" in Company Computers (January 8, 2008)
• Vancouver Resident Sentenced in Internet Fraud Case: Edwin Garcia Is Sentenced for Internet High-yield Investment Scam and Money Laundering (January 8, 2008)
• Former Assistant Bank Branch Manager Pleads Guilty to Fraud and Related Activity in Connection with Computers: Unauthorized $50,000 Deposit into Personal Account Was to Cover Gambling Losses (January 4, 2008)
• Alan Ralsky, Ten Others, Indicted in International Illegal Spamming and Stock Fraud Scheme (January 3, 2008)
Year 2006

- Utah Man Sentenced to 24 Months in Prison for Bringing Down Wireless Internet Services (December 14, 2006)
- California Man Sentenced for Recklessly Damaging a Protected Computer Owned by his Former Employer (October 16, 2006)
- Florida Man Sentenced for Causing Damage and Transmitting Threat to Former Employer's Computer System (July 13, 2006)
- Former Technology Manager Sentenced To A Year In Prison For Computer Hacking Offense (June 23, 2006)
- North Carolina Man Charged with Illegally Accessing American College of Physicians Database (June 15, 2006)
- Former Federal Computer Security Specialist Sentenced for Hacking Department of Education Computer (May 12, 2006)
- "Botherder" Dealt Record Prison Sentence for Selling and Spreading Malicious Computer Code (May 8, 2006)
- California Man Pleads Guilty in "Botnet" Attack That Impacted Seattle Hospital and Defense Department (May 4, 2006)
- United States Secret Service’s Operation Rolling Stone Nets Multiple Arrests (March 28, 2006)
- Telemarketing Firm Official Indicted in New Hampshire Phone Jamming Case (March 27, 2006)
- Former Federal Computer Security Specialist Pleads Guilty to Hacking Department of Education Computer (March 1, 2006)
• Cleveland, Ohio Man Sentenced to Prison for Bank Fraud and Conspiracy (February 28, 2006)
• Former Officer of Internet Company Sentenced in Case of Massive Data Theft from Acxiom Corporation (February 22, 2006)
• Grand Jury Returns Indictment Charging Student with Accessing Protected Computer at University of Utah (February 17, 2006)
• Utah Man Charged with Bringing Down Wireless Internet Services in Vernal Region (February 15, 2006)
• California Man Indicted for Botnet Attack That Impacted Hospital (February 10, 2006)
• Florida Man Indicted for Causing Damage and Transmitting Threat to Former Employer's Computer System (February 7, 2006)
• Azusa, California "Phisher" Arrested for Posing as America Online Billing Representative and Obtaining Personal Information from Subscribers (January 26, 2006)
• Bot Herder Pleads Guilty to Fraudulent Adware Installs and Selling Zombies to Hackers and Spammers (January 23, 2006)
• Dayton, Ohio, Man Pleads Guilty to Sexual Exploitation Crimes Involving Minors and Computer Intrusion (January 19, 2006)

Year 2005
• Man Pleads Guilty to Infecting Thousands of Computers Using Worm Program then Launching them in Denial of Service Attacks (December 28, 2005)
• Silicon Valley Engineer Indicted for Stealing Trade Secrets and Computer Fraud (December 22, 2005)
• Former RNC New England Regional Director Convicted in New Hampshire Phone Jamming Case (December 15, 2005)
• Plano Man Convicted of Computer Sabatage (November 21, 2005)
• Six Defendants Plead Guilty in Internet Identity Theft and Credit Card Fraud Conspiracy (November 17, 2005)
• Computer Virus Broker Arrested for Selling Armies of Infected Computers to Hackers and Spammers (November 3, 2005)
• Houston Man Pleads Guilty to Federal Identity Theft Charges, Says Justice Department (November 1, 2005)
• Massachusetts Teen Convicted for Hacking into Internet and Telephone Service Providers and Making Bomb Threats to High Schools in Massachusetts and Florida (September 8, 2005)
• Federal Jury Convicts Former Technology Manager of Computer Hacking Offense Defendant Found Guilty of Placing Computer "Time Bomb" On Employer's Network Following Employment Dispute (September 8, 2005)
• Creator and Four Users of Loverspy Spyware Program Indicted (August 26, 2005)
• Justice Department Announces Conviction of Florida Man Accused of Massive Data Theft from Acxiom, Inc. (August 12, 2005)
• Disgruntled Phillies Fan/Spammer Sent to Prison for Four Years (July 14, 2005)
• Former Computer Science Graduate Student Sentenced for Hacking Major Corporations (April 25, 2005)
• Fairlawn, Ohio Man Sentenced in e-Bay Auction Scam (March 28, 2005)
• New York Teen Pleads Guilty to Making Extortion Threats Against Internet Company (March 22, 2005)
• Pleasant Hill, California Computer Hacker from "Deceptive Duo" Guilty of Intrusions into Government Computers and Defacing Websites (March 11, 2005)
• Queens Man Sentenced to 27 Months' Imprisonment on Federal Charges of Computer Damage, Access Device Fraud and Software Piracy (February 28, 2005)
• New York Spammer Arrested for Making Threats Against Internet Messaging Company and Sending More Than 1.5 Million Spam Messages (February 17, 2005)
• Former IT Manager of Software Firm Indicted on Computer Crime Charges (February 16, 2005)
• Juvenile Sentenced for Releasing Worm That Attacked Microsoft Web Site (February 11, 2005)
• Computer Hacker Who Victimized T-Mobile Pleads Guilty in Los Angeles Federal Court (February 15, 2005)
• Minnesota Man Sentenced to 18 Months in Prison for Creating and Unleashing a Variant of the MS Blaster Computer Worm (January 28, 2005)
• Former Sacramento Man Arrested in eBay Auction Scam (January 27, 2005)

Year 2004
• Hacker Sentenced to Prison for Breaking into Lowe's Companies' Computers with Intent to Steal Credit Card Information (December 15, 2004)
• Fourth Defendant in Massive Internet Scam Pleads Guilty to Fraud and Money Laundering Charges (November 18, 2004)
• Nineteen Individuals Indicted in Internet 'Carding' Conspiracy (October 28, 2004)
• CHIPS Unit Established in the Eastern District of California United States Attorney Office (October 19, 2004)
• Ex-Official of Manhattan Computer Consulting Firm Pleads Guilty to Computer Attack Charge (September 9, 2004)
• California Man Admits Hacking Into Computers of High-Technology Company (August 31, 2004)
• Former Employee of a Massachusetts High-Technology Firm Charged with Computer Hacking (August 23, 2004)
• Six Internet Fraudsters Indicted in International Conspiracy to Steal More Than $10 Million From World's Largest Technology Distributor (August 4, 2004)
• Vallejo, California Woman Admits to Embezzling More Than $875,035 (July 28, 2004)
• Florida Man Charged with Breaking into Acxiom Computer Records (July 21, 2004)
- China Citizen Pleads Guilty to Unauthorized Access of a Software Company with Intent to Defraud (July 7, 2004)
- Seattle, Washington Man Arrested for Hacking into Internet Search Engine Alta Vista (July 2, 2004)
- Cary Waage Sentenced to Prison for his Role in $60 Million Internet Scam (July 9, 2004)
- Wi-Fi Hacker Pleads Guilty to Attempted $17,000,000 Extortion (June 8, 2004)
- Vallejo, California Woman Charged with Exceeding Authorized Computer Access to Embezzle More Than $875,035 (May 27, 2004)
- Fraudster Sentenced to Nearly Four Years in Prison in Internet 'Phishing' Case: Spammer Posed as AOL and Paypal to Con Customers into Providing Personal Information (May 18, 2004)
- Pennsylvania Man Sentenced to Prison for Accessing Massachusetts Investor's On-line Investment Account and Making $46,000 in Unauthorized Trades (May 5, 2004)
- Department of Justice Announces Arrests of Detroit-Area Men on Violations of the "Can-Spam" Act (April 29, 2004)
- Parma, Ohio Man Indicted for Ebay Fraud, Credit Card Fraud, and Identity Theft (April 28, 2004)
- Former Global Crossing Employee Sentenced to 46 Months in Prison for Posting Thousands of Social Security Numbers and Multiple Threats on his Internet Website (April 16, 2004)
- Orange County, California Man Indicted on Wiretapping Charges for Installing Spy Hardware on Employer's Computer (March 23, 2004)
- Oak Park, California Computer Programmer Arrested for Extortion and Mail Fraud Scheme Targeting Google, Inc. (March 18, 2004)
- Mission Viejo, California Teen Guilty in Internet Auction Fraud; Defendant Also Admits $400,000 Bank Fraud (March 1, 2004)
• Sewell, New Jersey Man Sentenced to 37 Months in Prison for Defrauding eBay Bidders and Cashing Checks from Stolen Mail (February 27, 2004)
• 'Cyberscammer' Sentenced to 30 Months for Using Deceptive Internet Names to Mislead Minors to X-Rated Sites (February 26, 2004)
• Former Employee of Viewsonic Sentenced to One Year for Hacking into Company's Computer, Destroying Data (February 23, 2004)
• Louisiana Man Arrested for Releasing 911 Worm to WebTV Users (February 19, 2004)
• Two California Men Indicted for Unlawfully Obtaining Credit Information, Attempted Credit Fraud (February 10, 2004)
• Former Employees of Dallas-based Car Parts Distributorship Charged with Repeatedly Intruding into Competitor's Computer Database for Commercial Advantage and Illegally Trafficking in Computer Passwords. (February 9, 2004)
• Man Pleads Guilty to Gaining Unauthorized Access and Recklessly Damaging Computers of Several High-Technology Companies Including eBay and Qualcomm From His Graduate School Dorm Room (January 29, 2004)
• Hacker Pleads Guilty in Manhattan Federal Court to Illegally Accessing New York Times Computer Network (January 8, 2004)
• Mississippi Man Indicted for Attempted Extortion of $2.5 Million from Best Buy Co., Inc. (January 6, 2004)

Year 2003
• Milford, Ohio Man Pleads Guilty to Hacking (December 18, 2003)
• Former Hellmann Logistics Computer Programmer Sentenced for Unauthorized Computer Intrusion (December 5, 2003)
• Former Global Crossing Employee Convicted of Posting Threats on His Internet Website and Distributing Information to be Used in Identity Theft (December 4, 2003)
• Former Employee of American Eagle Outfitters Sentenced to Prison for Password Trafficking and Computer Damage (December 2, 2003)
• Three Men Indicted for Hacking into Lowe's Companies' Computers with Intent to Steal Credit Card Information (November 20, 2003)
• Two Alleged Computer Hackers Charged in Los Angeles as Part of Nationwide 'Operation Cyber Sweep' (November 20, 2003)
• Sewell, New Jersey Man Admits to Defrauding eBay Bidders and Cashing Checks From Stolen Mail (November 18, 2003)
• Dallas, Texas FBI Employee Indicted for Public Corruption (November 5, 2003)
• Disgruntled Philadelphia Phillies Fan Charged with Hacking into Computers Triggering Spam E-mail Attacks (October 7, 2003)
• Former Employee of Viewsonic Pleads Guilty to Hacking into Company's Computer, Destroying Data (October 6, 2003)
• President of San Diego Computer Security Company Indicted in Conspiracy to Gain Unauthorized Access into Government Computers (September 29, 2003)
• Juvenile Arrested for Releasing Variant of Blaster Computer Worm That Attacked Microsoft (September 26, 2003)
• Chicago Man Pleads Guilty to MSN Internet Fraud (September 12, 2003)
• Southern California Man Pleads Guilty to Fraud in Online Escrow Scam (September 5, 2003)
• Minneapolis, Minnesota 18 year old Arrested for Developing and Releasing B Variant of Blaster Computer Worm (August 29, 2003)
- Former Chairman of the Republican Party of Virginia Pleads Guilty and is Sentenced for Wiretapping-Related Violation (August 12, 2003)
- Sacramento, California Woman Convicted of Embezzling More Than $910,000 In Computer Fraud Scheme (August 1, 2003)
- Russian Man Sentenced for Hacking into Computers in the United States (July 25, 2003)
- FBI Employee Arrested and Charged in Three Federal Indictments (July 17, 2003)
- Kazakhstan Hacker Sentenced to Four Years Prison for Breaking into Bloomberg Systems and Attempting Extortion (July 1, 2003)
- Southern California Man Who Hijacked Al Jazeera Website Agrees to Plead Guilty to Federal Charges (June 12, 2003)

- Computer Hacker Sentenced to One Year and One Day And Ordered to Pay More than $88,000 Restitution For Series of Computer Intrusions and Credit Card Fraud (June 12, 2003)
- Leader of $60 Million Internet Scam Pleads Guilty to Fraud and Money Laundering Charges (May 16, 2003)
- Three Californians Indicted in Conspiracy to Commit Bank Fraud and Identity Theft (May 12, 2003)
- Ex-employee of Airport Transportation Company Guilty of Hacking into Company's Computer (April 18, 2003)
- Student Charged with Unauthorized Access to University of Texas Computer System (March 14, 2003)
- St. Joseph, Missouri Man Pleads Guilty in District's First Computer Hacking Conviction (March 13, 2003)
- Computer Hacker Pleads Guilty to Computer Intrusion and Credit Card Fraud (March 13, 2003)
• California Woman Convicted for Unauthorized Computer Access to Customer Account Information in Credit Union Fraud Prosecution (March 10, 2003)
• Los Angeles, California Man Sentenced to Prison for Role in International Computer Hacking and Internet Fraud Scheme (February 28, 2003)
• Former Employee of American Eagle Outfitters Indicted on Charges of Password Trafficking and Computer Damage (February 26, 2003)
• U.S. Convicts Kazakhstan Hacker of Breaking into Bloomberg L.P.’s Computers and Attempting Extortion (February 26, 2003)
• Ex-employee of Airport Transportation Company Arrested for Allegedly Hacking Into Computer, Destroying Data (February 20, 2003)
• Vista, California Man Charged in Complex Internet Facilitated Wire Fraud Scheme (February 13, 2003)
• Ohio Man Attacked NASA Computer System Shutting Down Email Server (February 13, 2003)
• Former Employee of Viewsonic Arrested on Charges of Hacking into Company's Computer, Destroying Data (February 6, 2003)
• Pittsburgh, Pennsylvania Man Convicted of Hacking a Judge's Personal E-Mail Account (January 23, 2003)
• Alleged Leaders of $60 Million Internet Scam Indicted on Fraud and Money Laundering Charges (January 3, 2003)

Year 2002
• St. Joseph, Missouri Man Charged in Western District's First Computer Hacking Indictment (December 20, 2002)
• Man Indicted on Charges of Defrauding Buyers Using eBay Internet Auction Service, Remains Fugitive (December 20, 2002)
• Two Los Angeles, California, Men Accused of Operating Websites Selling Fake IDs Named in Conspiracy; 5 Felons Who Applied for Bogus Documents also Charged (December 20, 2002)
• U.S. Arrests Queens, New York, Man on Computer Fraud Charges (December 20, 2002)
• Disgruntled UBS PaineWebber Employee Charged with Allegedly Unleashing "Logic Bomb" on Company Computers (December 17, 2002)
• U.S. Announces What is Believed the Largest Identity Theft Case In American History; Losses are in the Millions (November 25, 2002)
• Hacker Plead Guilty to Attacks on San Diego Auto Site (November 15, 2002)
• British National Charged with Hacking Into N.J. Naval Weapons Station Computers, Disabling Network After Sept. 11; Indictment Also Filed in Virginia For Other Military Intrusions (November 12, 2002)
• Florida Lawyer Charged in Offshore Sports Betting Case (October 22, 2002)
• Melvern, Ohio Man Sentenced for Defrauding Bidders on eBay (October 16, 2002)
• Russian Computer Hacker Sentenced to Three Years in Prison (October 4, 2002)
• Sacramento, California, Woman Convicted of Committing Check 'Kite' Through Unauthorized Computer Access (September 17, 2002)
• Los Angeles, California Woman Admits Bilking eBay Bidders (September 10, 2002)
• San Gabriel Valley, California Man Pleads to Illegally Accessing Former Employer's Computers (September 9, 2002)
• Defendant Sentenced in Three Fraud Prosecutions for Online Auction, Telemarketing, and Computer-Generated Counterfeit Check Scams (August 30, 2002)
• Former LA Ram Sentenced in eBay Internet Fraud Schemes (August 5, 2002)
• San Fernando Valley Residents Indicted in Scheme to Hack Into Software Firm Computer and Delete $2.6 Million Project (August 2, 2002)
• Fairfax, Virginia Man Sentenced 144 Months for Internet Auction Fraud (July 16, 2002)
• Internet Auction Scam Results in Guilty Plea (July 8, 2002)
• San Francisco Man Sentenced for Selling Fake Derek Jeter and Normar Garciaparra Baseball Bats on eBay (July 2, 2002)
• Owner of Internet Service Provider Sentenced to 18 Months in Prison for Credit Card Scam (June 10, 2002)
• Melvern, Ohio Man Indicted for eBay Auction Fraud (June 5, 2002)
• Internet Doctor Sentenced to Over 4 Years in Prison (May 29, 2002)
• Two Kazakhstan Citizens Accused of Breaking Into Bloomberg L.P.’s Computer and Extortion are Extradited (May 21, 2002)
• Defendant Pleads Guilty in Three Fraud Prosecutions for Online Auction, Telemarketing, and Computer-Generated Counterfeit Check Scams (May 17, 2002)
• Twenty-Seven Month Sentence in Internet Fraud Scheme to Defraud Priceline.Com and Others; Unauthorized Computer Access Conspiracy (May 17, 2002)
• Former Chief Technology Officer Arrested for Computer and Voicemail System Intrusions; Transmitting Threats Via the Internet (May 16, 2002)
• Reynoldsburg, Ohio Man Sentenced for Misuse of Law Enforcement Computer (May 8, 2002)
• Green Bay, Wisconsin Man Charged with Computer Intrusion, Software Piracy and Numerous Destructive Acts (May 7, 2002)
• San Jose, California Man Pleads Guilty to Selling Explosives on eBay (May 2, 2002)
• Creator of Melissa Computer Virus Sentenced to 20 Months in Federal Prison (May 1, 2002)
• U.S. Charges Engineer with Computer Intrusion, Destruction of Database at Manhattan Apparel Company (April 26, 2002)
• Man Pleads Guilty to Unauthorized Access of Las Vegas Medical Imaging Computer System (April 17, 2002)
• Computer Operator Sentenced or Breaking Into Ex-Employer’s Database (March 27, 2002)
• Parma, Ohio Man Indicted for Unauthorized Access into Computer System of Alltel Communications, Inc.; Threatening E-Mails (March 26, 2002)
• Five Guilty Pleas and Seven Arrested for Wire and Securities Fraud in Connection with Collapse of Apponline.com (March 12, 2002)
• CHIPs Unit Established in the Eastern District of California United States Attorney Office (March 5, 2002)
• Man Sentenced for eBay Auction Fraud of Certain Rare Baseball and Basketball Card Sets (March 4, 2002)
• Former Computer Network Administrator at New Jersey High-Tech Firm Sentenced for Unleashing $10 Million Computer “Time Bomb” (February 26, 2002)
• Former Chase Financial Corp. Employees Sentenced for Scheme to Defraud Chase Manhattan Bank and Chase Financial Corporation (February 19, 2002)
• Internet Doctor Convicted in Oklahoma City (January 30, 2002)
• Six Defendants Sentenced in $16 Million Bogus Investment Scheme Marketed Over Internet (January 30, 2002)
• San Francisco Man Pleads Guilty to Unauthorized Access of Catholic Healthcare West Computer Causing Damage (January 18, 2002)
• CHIPs Unit Established in the Eastern District of Virginia United States Attorney Office (January 14, 2002)
## APPENDIX - III
### INDIAN FRAUDS FROM 2002 TO 2010

<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>Case</th>
<th>Date</th>
<th>Transaction</th>
<th>Type</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Karan Bahree used to work at Infinity eSearch, New Delhi, sold top secret information on 1,000 Britons bank accounts for just £3 each to the Sun</td>
<td>August 2002</td>
<td>£3 for each account</td>
<td>ID Theft</td>
<td>Violations of requirement 3 &amp; 4 of PCI-DSS 1.2</td>
</tr>
<tr>
<td>2.</td>
<td>Shekhar Verma, an IIT Kharagpur graduate and a former employee of software firm Geometric Software Solutions Ltd, GSSL, was caught red-handed trying to sell a data source code, was the property of GSSL’s American client Solidworks</td>
<td>August 2002</td>
<td>$240,000 for the code</td>
<td>ID Theft</td>
<td>Violations of requirement 3 &amp; 4 of PCI-DSS 1.2</td>
</tr>
<tr>
<td>3.</td>
<td>Two employees of IntelNet Global Service, a BPO firm, had hacked into TransUnion’s database in August 2005 on the instructions of one Frederick Rodney, based in the US. provided file numbers of hundreds of card holders, and had asked the employees to make the changes in their financial profiles.</td>
<td>August 2005</td>
<td>paid over Rs 10 lakh</td>
<td>Hacking</td>
<td>Violations of requirement 3, 4 &amp; 10 of PCI-DSS 1.2</td>
</tr>
<tr>
<td>4.</td>
<td>Shaikh working in the Credit Card department of State Bank of India had access to credit card details of customers, which he passed</td>
<td></td>
<td>Credit card Fraud</td>
<td></td>
<td>Violations of requirement 10 &amp; 11 of PCI-DSS 1.2</td>
</tr>
</tbody>
</table>
on to his friend kale who further passed on to his friend Lukkad who used this information to book air tickets.

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>5.</strong> Two Nadar brothers along with their friend Ramesh Gala, took help of SMS technology and launched the first of it’s kind SMS fraud in India. They launched a campaign in print media &amp; also put up a website (<a href="http://www">www</a>. getpaid4sms. com) wherein subscribers were asked to pay deposit of INR 500 and they receive 10 SMS every day against it. The customers were promised handsome commissions if they managed to rope in more subscribers by forwarding the messages.</td>
<td>Rs.400 million</td>
<td>Internet Fraud</td>
</tr>
</tbody>
</table>

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>6.</strong> Kamal Kumar, with assistance from his friend in Nigeria, develops a clone of the ICICI website (original - <a href="http://www.icicibank.com">www.icicibank.com</a>; clone - <a href="http://www">www</a>. icicibank.net) E-mails are sent by Kumar to ICICI customers, asking them to validate their details like credit card numbers, account numbers, banking passwords etc. Link at the bottom of emails would lead customers to the fake website. Details are used by Kumar to do</td>
<td>Feb. 2006</td>
<td>Phishing</td>
</tr>
</tbody>
</table>
shopping on the net, for which the real card holder ended up paying.

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>7.</td>
<td>Debasish Pandit, a computer hardwire service provider, and constable Rabi Narayan Sahu were buying goods online using credit cards that belonged to others. They obtained information of about 700 to 800 international credit cards by hacking</td>
<td>Jan. 13, 2007</td>
</tr>
<tr>
<td>8.</td>
<td>Rajesh, a resident of Ambalamukku, runs an Internet cafe at Chenthitta. After befriending the engineer through chat, Rajesh posed as 'Renuka' and used a voice converter to disguise his voice. He later forwarded a photo from a marriage bureau to the engineer, who provided a credit card and code to 'Renuka' to withdraw Rs2,500 for purchasing a flight ticket to Mumbai. The engineer even booked a room for 'Renuka' who failed to turn up. Enquiries revealed that Rs22,000 was withdrawn using the credit card</td>
<td>4 March 2007</td>
</tr>
<tr>
<td>9.</td>
<td>Shaikh was working in the credit card department; due to this he had access to credit card details of some customers. He gave that</td>
<td>Feb. 28, 2007</td>
</tr>
</tbody>
</table>
information to Kale. Kale in return passed this information to his friend Lukkad. Using the information obtained from Kale Lukkad booked tickets. He used to sell these tickets to customers and get money for the same. He had given few tickets to various other institutions. It is found that details misused were belonging to 100 people.

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>10.</td>
<td>Vinset Mezek (26), Ogobol Tony (25), Kovhni Okosav (35), Charles Niogo (21) and Odirom Babatude (26) used to sent mails to people about vacancies in hotels outside India. If anyone responded, they would ask him to deposit money in their bank accounts in Mumbai. However, once they received the money, they would never contact the person.</td>
<td>06 March 2007</td>
<td>Rs 1.2 lakh</td>
</tr>
<tr>
<td>11.</td>
<td>Pankaj Sharma who said that he won an auction for a mobile phone online from a seller whose id was enlisted in a well-known shopping site, eBay.com. He also told that he had paid by his credit card. But even after ten days he did not receive the mobile. Tarang Bhargava, a web designer for e-marketing had</td>
<td>11 Aug. 2007</td>
<td>Rs 36.5 crore</td>
</tr>
<tr>
<td></td>
<td>fraudulently misused his name and account</td>
<td>Nov. 30</td>
<td>Rs 400 million</td>
</tr>
<tr>
<td>---</td>
<td>------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
</tr>
<tr>
<td>12.</td>
<td>Jayanand Nadar, 30, and Ramesh Gala, 26, the duo launched an aggressive and catchy advertisement campaign in the print media that read: “Nothing is impossible. The word itself is: I M Possible.” As part of the attractive scheme, the Nadar brothers messaged random numbers, asking people interested in ‘earning Rs.10,000 per month’ to contact them. &quot;Interested 'subscribers' were asked to deposit Rs.500 each. The conmen duo claimed o be working with a US-based company named Aropis Advertising Company, which wanted to market its client's products through SMS'.”. The brothers even put up a website (http:// <a href="http://www.getpaid4sms.com/">www.getpaid4sms.com/</a>) to promote their scheme. Subscribers who registered with them received about 10 SMS' every day about various products and were promised handsome commissions if they managed to rope in more subscribers by forwarding the messages,” In return, the</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Nadars promised to pay Rs.10,000 over 16 months to the investors. The amount was to be paid in instalments of Rs.1,000 every few months.

The brothers are said to have told the subscribers that their American clients wanted to conduct a study about local response to their advertisement and were using SMS as it was the latest medium of communication.

The duo invited people to become agents and get more members for the scheme. Gala reportedly looked after the accounts.

Initially, the brothers paid up small amounts. But when cheques and pay orders of larger sums issued by the duo were not honoured, the agents got worried. The SMSes too suddenly stopped.

13. Mailform is a service of PC Svet, which is a part of the Czech company PES Consulting. The Webmaster of the site is a person named Petr Stastny. A URL on Geocities that is almost a facsimile version of the UTI Bank's home page is reported.

| Phishing | Violations of requirement 1 & 4 of PCI-DSS 1.2 |
to be circulating amongst email users. The web page not only asks for the account holder's information such as user and transaction login and passwords, it has also beguilingly put up disclaimer and security hazard statements."

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>14.</td>
<td>Debasis Pandit, a BCA student, Rabi Narayan Sahu, his associate and a constable of Rourkela, allegedly hacked into the eBay India site and gathered the details of around 700 credit cardholders. He then made purchases by using their passwords. Pandit used the address of Sahu for delivery of the purchased goods, said police. The gang was involved in train, flight and hotel reservations.</td>
</tr>
<tr>
<td>15.</td>
<td>Five hackers hacked into different accounts the victim was using the provided by the net banking services of Punjab National Bank. Officials say, that this bank unlike others does not send any intimation to the account holder when money is transferred from one account to another. They either used the money that was temporarily transferred to</td>
</tr>
<tr>
<td>ID</td>
<td>Case Description</td>
</tr>
<tr>
<td>-----</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>16</td>
<td>Edward Burns, senior executive of a leading BPO firm, EXL Solutions, which contracted work of leading British insurance firm Aviva. After opening accounts under fake names, Burns, instead of transferring the insurance claim amounts to the actual insurers, credited the amount into these fraudulently created bank accounts.</td>
</tr>
<tr>
<td>17</td>
<td>In Canada fraudsters defrauded the bank by discovering houses with lower values than others. Then they found people whom they paid $3,000 to $8,000 each to sign on mortgage papers and become fake owners. Then the fraudsters would inflate income of these fake buyers to get mortgage applications approved. Once the bank approved the mortgage, the fraudsters sent the money abroad. The Indian-born Canadian MP Devinder Shory, has been named in the lawsuit case as the lawyer for four mortgages.</td>
</tr>
<tr>
<td>18</td>
<td>Yogendra Singh, an engineer, received a call from an</td>
</tr>
</tbody>
</table>
unidentified caller who introduced him as a customer care executive from a leading bank. Singh had a Citibank credit card. "Asking if I would want a Standard Chartered Bank's credit card, the caller took down details, such as my date of birth, mother's name and the last two digits of my Citibank card. The next day, another man came and collected documents supporting these details and said I would get a new credit card," A few days later, he received another call and this time, the man posed as Citibank employee. He asked Singh if he would like to increase the credit limit on his card. "Even after a week, when no one from Citibank did not contact me about the credit limit, I tried to log on to my bank account, but failed. It was hacked," Singh told the police. Singh called up the customer care service and learnt that his password had been changed and Rs 82,940 had been transferred from his account to pay Reliance Energy bills of several people. The ATS traced the IP address to Ashish Cyber Cafe.
in Kandivli and instructed the owner, Ashraf, to keep a tab on the suspect, Aurangzeb. Ashraf checked CCTV images in his cafe and a few weeks later, when he spotted the man, he alerted a Dahisar police station's constable who detained Aurangzeb.

<table>
<thead>
<tr>
<th>19.</th>
<th>In Tripura two youths had deposited the money into two separate private banks following the anonymous messages asking for the amount as processing fee for an online lottery worth millions of dollars. After that, those sending the messages remained silent.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Feb. 2009</td>
</tr>
<tr>
<td></td>
<td>Online Fraud</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>20.</th>
<th>Burns, 30, an Indian citizen, was working in the insurance claims division of EXL, which contracted work of leading British insurance firm Aviva. After opening accounts under fake names, Burns, instead of transferring the insurance claim amounts to the actual insurers, credited the amount into these fraudulently created bank accounts.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Feb. 16th, 2009</td>
</tr>
<tr>
<td></td>
<td>Online Fraud</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>21.</th>
<th>Mr. Saiyed Taherali Kalumiya (Resi address-Village Gothada Baroda ) is having account with Bank of Baroda</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>22nd July 2009</td>
</tr>
<tr>
<td></td>
<td>ATM fraud</td>
</tr>
</tbody>
</table>
which is located near old bus stand, of Savli Taluka, Baroda. Mr. Taherali have applied for ATM card but still Bank have not issued ATM card to him. When Mr. Taherali required money he walked in a bank to withdraw Rs 5000/- by cheque. Bank Manager informed that he is not having sufficient amount in his account. On this information Mr. Taherali said he has deposited more that required amount in Bank. When further inquiry was done, Bank Manager said that Mr. Taherali have withdrawn Rs 10000/- on 4th August and Rs 10000/- on 6th August by ATM Card.

| 22. | Four members of a gang, including an engineering student, who were using fake credit cards to withdraw money from the accounts of customers. The kingpin of the gang used to get the details of credit cards of foreign customers through his friends living abroad. He would then prepare fake credit cards and transfer the details of genuine credit cards on to them. After preparing the fake credit card, he along with his three | 22nd Aug. 09 | Rs 80 lakh | Credit card fraud & Id theft | Violations of requirement 3, 4 & 10 of PCI-DSS 1.2 |
|      |  |  |  |  |  |

Violations of requirement 3, 4 & 10 of PCI-DSS 1.2
associates would make purchases and also withdraw money from ATM centres. Sources said a electronic gadget used to transfer the customer data onto the fake credit cards and a computer.

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>23.</td>
<td>The first gang, Ramanand Yadav, Adil Jehan Kapadia and Tanveer alias Jolly Asif Ali Khan, set up a fake company in the name of ACIL Industries and had even rented an office and opened a website to attain credibility and applied for loans under fake names, Whereas the members of the second gang would break open cheque drop boxes in ATMs and banks and forge them. The accused had used the fake documents to apply for loans in the names of seven persons and duped a bank of Rs 29.5 lakh</td>
<td>Feb. 2009</td>
<td>Rs 30 lakh</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24.</td>
<td>I Ibrahim Ansari of Mumbai, steal the id and passwords of Madurai-based engineer V Saravanan by phishing email or by planting malicious software. They recruit accomplices or couriers through social networking sites. They then get details of the couriers and transfer</td>
<td>August 2009</td>
<td>Rs 75,510</td>
</tr>
</tbody>
</table>

Violations of requirement 10 & 11 of PCI-DSS 1.2

Violations of requirement 1 & 4 of PCI-DSS 1.2
<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Bank or Account Details</th>
<th>Date</th>
<th>Amount</th>
<th>Type</th>
<th>Violations of Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>25.</td>
<td>Siddhartha Daga, vice-president (eastern region) of Indiabulls,</td>
<td>In just 45 minutes during the first hour of trading on August 6, Daga is accused of having sold off or diverted to his own account every single share that Arunabha Chakraborty owned. Chakraborty suffered a loss of Rs 46 lakh.</td>
<td>August 2009</td>
<td>Rs 1 Crore</td>
<td>Identity theft</td>
<td>Violations of requirement 3, 4 &amp; 10 of PCI-DSS 1.2</td>
</tr>
<tr>
<td>26.</td>
<td>Shyamsunder Sharma had a bank account with the Industrial Branch of Union Bank of India with a balance of Rs7 lakh, The account holder was on vacation and when he returned, he got the shock of his life after his account showed a zero balance. Rs7 lakh was transferred to different accounts of various banks in the city</td>
<td>22 Oct. 2009</td>
<td>Rs7 lakh</td>
<td>Identity theft</td>
<td>Violations of requirement 2 &amp; 4 of PCI-DSS 1.2</td>
<td></td>
</tr>
<tr>
<td>27.</td>
<td>Adwait Kulkarni, who works as divisional manager at Tata Motors and wife Anushree received a call from the ICICI bank staff informing her that a withdrawal of Rs 66,000 had taken place from my account. The transaction details</td>
<td>Dec. 11, 2009</td>
<td>Rs 66,000</td>
<td>Phishing</td>
<td>Violations of requirement 1 &amp; 4 of PCI-DSS</td>
<td></td>
</tr>
</tbody>
</table>
showed that Rs 50,000 was transferred into the account of one Richa Basnet in Delhi and Rs 16,000 in the account of one Narayan Trad-ers in Indore. The personal banking details entered by the person reaches straight to the fraudster. Kulkarni may also have re-ceived such an email.

| 28. | ICICI Bank initiated Scheme last year for savings bank accounts holders. Under it, an account holder can transfer cash to acquaintances who do not possess an ICICI card. The account holder has to link up his cellular phone number with his or her Internet banking account. Two beneficiaries' numbers may also be similarly linked. A maximum Rs 25,000 may be thus transferred in a day. Sachin Khampriya, posing as an ICICI Bank representative, approached Vidisha-resident Pokhanlal Sahu and managed to obtain secret details of the latter's account and a password. Khampriya then transferred Rs 7 lakh to Chhatarpur-resident Surekha Jain's account. He then met Ms Jain and managed to obtain details of her account | 4 Dec. 2009 | Rs 3 lakh | Data theft | Violations of requirement 3, 4 & 10 of PCI-DSS 1.2 |
271

| 29. | The website of the “Rashtriya Vigyan Kendra” claims it to be a government enterprise. Job aspirants have been told to send Rs 200 as application fee for 190 jobs advertised in local newspapers in Uttar Pradesh and neighbouring Uttarakhand. Application forms are also available on the website. The data has been almost lifted verbatim… from the website of Nehru Science Centre, Mumbai and other National Council of Science Museums (NCSM) branches, | Jan. 12, 2010 | Online Fraud | Violations of requirement 10 & 11 of PCI-DSS 1.2 |
| 30. | Soman Sundaram, Sham Sundrin and Mohammad Naujeen, residents of Chandigarh were actively involved in online trading of gold, silver, oil products and various other articles illegally and claimed to have the approval of the Reserve Bank of India for conducting the business | Feb. 24, 2010 | Rs 5.1 lakh | Online Fraud | Violations of requirement 10 & 11 of PCI-DSS 1.2 |
| 31. | S Vinayak Shivaji Khandare (20) and I Ibrahim Ansari (25), two Mumbai men for withdrawing Rs 26.55 lakh | 24 May 2010 | Rs 27 lakh | Identity Theft | Violations of requirement 3, 4 & 10 of |
and Rs 75,510 respectively through fraudulent means from two separate accounts of two Tamil Nadu-based persons using net banking.

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>32.</td>
<td>Shaileshkumar P Jain, Bjorn Daniel Sundin, owned and operated Innovative Marketing Inc (IM), a company registered in Belize that purported to sell anti-virus and computer performance/repair software through the internet and that operated a subsidiary called Innovative Marketing Ukraine, located in Kiev. deceived Internet users into falsely believing that their computers were infected with &quot;malware&quot; or had other critical errors to induce them to purchase &quot;scareware&quot; software products that had limited or no ability to remedy the purported, but nonexistent, defects. The trio placed fake advertisements about their products on various legitimate companies’ websites. The victim companies allegedly were defrauded of at least US $85,000 in unpaid fees promised by the fictitious ad agencies. Unknown to the victim companies, the internet</td>
<td>May 28, 2010</td>
</tr>
</tbody>
</table>
ads that were placed on their websites by these fictitious agencies contained hidden computer code that "hijacked" the Internet browsers of individual victims, redirecting their computers without their consent to websites controlled by Sudin and Jain. The victims were then prompted with a series of error messages claiming that the user's computer was experiencing a critical error and the victim needed to purchase an IM-distributed software product to remedy the problem. Reno 26, of Ohio owned and operated the former Byte Hosting Internet Services, which operated call centers that provided technical and billing support to victim consumers on behalf of IM.
## APPENDIX – IV
### HISTORY OF CREDIT CARD

<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>Brief history of credit/debit card</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>The idea of the credit card was first introduced in a book titled “Looking Backward,” and 1887 novel by Edward Ballamy.</td>
<td>1887</td>
</tr>
<tr>
<td>2.</td>
<td>Charge cards, as they were first called, were originally used for buying gasoline during the 1920’s. Theses charge cards were printed on paper cards and were very easy to forge</td>
<td>1920</td>
</tr>
<tr>
<td>3.</td>
<td>Charge Plate which was a small piece of metal and had the owners name and address printed on it as well as a small piece of card for the users signature. The Charge Plate emerged in the 1930’s and was usually kept at the store and only issued by the larger companies to their most regular customers.</td>
<td>1930</td>
</tr>
<tr>
<td>4.</td>
<td>Diners Club card. Founded in 1950 by Frank X. McMcNamara and Ralph Schneider, the Diners Club issued a card that allowed people to use it instead of various other cards. This card required to pay the entire balance each month.</td>
<td>1950</td>
</tr>
<tr>
<td>5.</td>
<td>American Express led to the creation of a global credit card system. In 1958 the Visa system came into existence via Bank of Americas BankAmericard.</td>
<td>1958</td>
</tr>
<tr>
<td>6.</td>
<td>MasterCard came into the world in 1966 and was first known as MasterCharge.</td>
<td>1966</td>
</tr>
<tr>
<td>7.</td>
<td>U.K., the first country to release the credit card in 1966.</td>
<td>1966</td>
</tr>
<tr>
<td>Central bank</td>
<td>Reserve Bank of India</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------</td>
<td></td>
</tr>
<tr>
<td>Nationalised banks</td>
<td>Allahabad Bank · Andhra Bank · Bank of Baroda · Bank of India · Bank of Maharashtra · Canara Bank · Central Bank of India · Corporation Bank · Dena Bank · IDBI Bank · Indian Bank · Indian Overseas Bank · Oriental Bank of Commerce · Punjab &amp; Sind Bank · Punjab National Bank · Syndicate Bank · UCO Bank · Union Bank of India · United Bank of India · Vijaya Bank</td>
<td></td>
</tr>
<tr>
<td>Private banks</td>
<td>Axis Bank · Bank of Rajasthan · Bharat Overseas Bank · Catholic Syrian Bank · City Union Bank · Development Credit Bank · Dhanalakshmi Bank · Federal Bank · Ganesh Bank of Kurundwad · HDFC Bank · ICICI Bank · IndusInd Bank · ING Vysya Bank · Jammu &amp; Kashmir Bank · Karnataka Bank Limited · Karur Vysya Bank · Kotak Mahindra Bank · Lakshmi Vilas Bank · Nainital Bank · Ratnakar Bank · Rupee Bank · Saraswat Bank · SBI Commercial and International Bank · South Indian Bank · Tamilnad Mercantile Bank Limited · Yes Bank</td>
<td></td>
</tr>
<tr>
<td>Foreign bank</td>
<td>ABN AMRO · Abu Dhabi Commercial Bank · Antwerp Diamond Bank · Arab Bangladesh Bank · Bank International Indonesia · Bank of America · Bank of Bahrain &amp; Kuwait · Bank of Ceylon · Bank of Nova Scotia · Bank of Tokyo Mitsubishi UFJ · Barclays Bank · Citibank India · HSBC · Standard Chartered · Deutsche Bank · Royal Bank of Scotland</td>
<td></td>
</tr>
</tbody>
</table>
Regional Rural banks

Rural banks: North Malabar Gramin Bank · South Malabar Gramin Bank · Pragathi Gramin Bank · Shreyas Gramin Bank

Financial Services: Real Time Gross Settlement (RTGS) · National Electronic Fund Transfer (NEFT) · Structured Financial Messaging System (SFMS) · CashTree · Cashnet · Automated Teller Machine (ATM)
# APPENDIX – VI

## QUESTIONNAIRE ON CREDIT / DEBIT CARD HOLDERS

**Date:**

<table>
<thead>
<tr>
<th>Name of the Respondent</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Dept/College Name:</td>
<td></td>
</tr>
<tr>
<td>Address:</td>
<td></td>
</tr>
<tr>
<td>Qualifications: PG/Doctorate/Graduate/Other:</td>
<td></td>
</tr>
<tr>
<td>Age: 15-25</td>
<td>26-40</td>
</tr>
<tr>
<td>Sex: Male</td>
<td>Female</td>
</tr>
<tr>
<td>Are you a Student /Faculty/ Research scholar/ other</td>
<td></td>
</tr>
<tr>
<td>Do you have credit card: yes, Name of the Bank:</td>
<td></td>
</tr>
<tr>
<td>Do you have debit card: if yes, Name of the Bank:</td>
<td></td>
</tr>
<tr>
<td>Kindly tick Y for Yes and N for No</td>
<td></td>
</tr>
<tr>
<td>Do you think your personal data is well protected by banks</td>
<td></td>
</tr>
<tr>
<td>Do you foresee frauds in ATM transaction</td>
<td></td>
</tr>
<tr>
<td>Can you use ATM without any technical problem?</td>
<td></td>
</tr>
<tr>
<td>Do you find difficulty in remembering PIN of your card?</td>
<td></td>
</tr>
<tr>
<td>Do you feel the ATM useful in withdrawing money?</td>
<td></td>
</tr>
<tr>
<td>Do you feel Menu on ATM are user friendly</td>
<td></td>
</tr>
<tr>
<td>Do you feel credit /debit card number is secured</td>
<td></td>
</tr>
<tr>
<td>Do you find Master/Visa/Maestro logo on your card</td>
<td></td>
</tr>
<tr>
<td>Do you use Kannada menu on ATM</td>
<td></td>
</tr>
<tr>
<td>Do you feel cards are safe to use in petrol bunk and super bazaar</td>
<td></td>
</tr>
<tr>
<td>Do you think banks are fully computerized to meet your expectations</td>
<td></td>
</tr>
<tr>
<td>Do you think RBI guidelines are strictly followed by banks</td>
<td></td>
</tr>
<tr>
<td>Do you think bank managers are well educated to address your credit/debit problems</td>
<td></td>
</tr>
<tr>
<td>Do you think purchasing products through online safe and secured</td>
<td></td>
</tr>
<tr>
<td>Do you think banks are transparent in their transactions?</td>
<td></td>
</tr>
<tr>
<td>Question</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>Do you think Nationalized banks are giving good services</td>
<td></td>
</tr>
<tr>
<td>Do you feel cyber frauds has increased after E-banking</td>
<td></td>
</tr>
<tr>
<td>Do you feel RBI has control over the foreign banks</td>
<td></td>
</tr>
<tr>
<td>Email-id : mob:</td>
<td></td>
</tr>
<tr>
<td>Signature :</td>
<td><strong>THANKYOU</strong></td>
</tr>
</tbody>
</table>
APPENDIX – VII

QUESTIONNAIRE ON PCI-DSS STANDARDS FOR CREDIT/DEBIT CARD HOLDERS

Dear Sir/ Madam

I, A M Sudhakara, Systems Engineer, University of Mysore doing research on E-security on Online Banking- Adoption of Security Standards for protecting Card Holders data. To pursue my research I need your cooperation in getting information in this regard. The given data will be confidential and will be used for only research purpose. The Questionnaire consists of PCI-DSS 12 points where the data security of all card holders is addressed.

Organization Details

Name of the Bank/Financial Institution/Organization

Address

Phone No: Fax No:

Email-Id :

Starting year :

Computerization started year

Do you issue credit card

[y/n]

Do you issue Debit card

[y/n]
No of card holders till to date:

No of cyber fraud reported so far


Up gradation of hardware/software once in 2 years [y][n]

Core banking [y][n]

Mobile banking [y][n]

No of ATM
APPENDIX - VIII
PSI- DSS Details - PCI DSS Version 1.2

Do you have firewall [y][n]
Do you have security policy [y][n]
Do you maintain computer services [y][n]
If no, do third party report maintenance on daily/ weekly/ monthly basis [y][n]
Do you set all the program defaults [y][n]
Do you restrict physical access to computer services [y][n]
Do you have encryption strategy [y][n]
Do you identify poorly coded applications [y][n]
Do you process scanning of data regularly [y][n]
Do you isolate customer data from other data [y][n]
Do you update POS applications regularly [y][n]
Do you maintain credit transactions in log files [y][n]
Do you update software with patches as they are released [y][n]
Do you employ third party to conduct an application test and code review to ensure security to data [y][n]
Do you implement strict SDLC processes [y][n]
Do you conduct user awareness and staff training regularly [y][n]
Do you monitor regularly intrusion and anomalies [y][n]
Do you hold people accountable for monitoring logs [y][n]
Do you watch the applications logs [y][n]
Do you have mobile commerce security [y][n]
Do you track all the access point in the organization [y][n]
Do you give unique ID for users [y][n]
Do your computer applications are secured [y][n]
Do you testing all the computer services regularly (hourly/daily/weekly/monthly/yearly) [y][n]
Do you follow PCI-DSS in your organization [y][n]
Do you follow RBI guidelines regularly [y][n]
Do you provide two factor authentication [y][n]
Do you provide bio-metrics for authentication [y][n]
Do you insure data for security breach [y][n]
Do you have credit/debit card redressal facilities at every branch [y][n]
Do you follow standard set by PCI-DSS in [y][n]

Signature of the respondent

Date:

Thank you for valuable participation and suggestions

* * * * *
1. Do you have a system for holding employees accountable for breaches in corporate security?  YES / NO
2. Do you monitor employee internet access?  YES / NO
3. Do you monitor or screen employee email?  YES / NO
4. Do you monitor or screen the transmission of key organizational documents that are transmitted outside of the company?  YES / NO
5. Are your “trusted” systems monitored for user access?  YES / NO
6. Do you employ the use of active security logging that monitors unauthorized user activity on your computer network?  YES / NO
7. Are your security logs strictly controlled? (Firewall logs, etc)  YES / NO
8. Is a senior corporate official directly responsible for the implementation of your organizational security policy?  YES / NO
9. Have you ever disciplined an employee due to malicious computer activity? (If yes, explain on attached page.)  YES / NO
10. Have you ever suspected an employee, subcontractor or consultant of conducting any form of malicious technical activity within your organization? (e.g., malicious computer activity, malicious wire or conversation intercept)  YES / NO
11. Have you experienced a burglary of any computer equipment within the past year? (If yes, explain on attached page.)  YES / NO
12. Do you perform employee reference or background checks prior to their employment?  YES / NO
13. Have you ever employed the professional services of any Computer Emergency Response Team (CERT) – or similar group - for the purpose of removing or investigating malicious computer activity on your network?  YES / NO
14. Is your organization responsible for the maintenance of your emergency power systems?  
15. Do you periodically inspect and test the operability of your emergency power systems?  
16. Are your security platforms maintained and updated by trained and certified security professionals?  
17. Were your security applications installed and configured by properly trained technical personnel?  
18. Is some form of user authentication implemented on your network?  
19. Would you be able to identify unauthorized user access to your network?  
20. Are there any remote access or remote maintenance capabilities to any portion of your network? (If yes, explain on attached page.)  
21. Are periodic technical security scans performed upon your network?  
22. Have you installed all the current application updates, security patches or associated “Hot Fixes” to all your operating systems (OS)?  
23. Were the patches/hot fixes received from known reliable sources?  
24. Do you lease, borrow or share any server space or other systems assets that reside on physical hardware which you do NOT own? (If yes, explain on attached page and identify them on your network diagram.)  
25. Has your organization ever had a comprehensive organizational, physical, technical and personnel security assessment?  
26. Do you have remote maintenance capabilities to any networked computer support equipment? (Faxes, copy machines, printers, etc.)  
27. Do you have physical security safeguards installed and working on your Network Operations Center (NOC)?
28. Did experienced and technically proficient professional(s) configure your network? [YES / NO]
29. Have you ever been unable to provide service to your customers due to a lack of electrical power to your networked systems? [YES / NO]
30. Has your network administrator been employed with your company for over one year? [YES / NO]
31. Is the access to your security logs strictly controlled? [YES / NO]
32. Do you maintain your security logs for over 180 days? [YES / NO]
33. Do you perform a weekly review of all your security logs? [YES / NO]
34. Have you ever experienced an unauthorized, external intrusion onto your network? (If yes, explain on attached page.) [YES / NO]
35. Has an internal malicious user ever gained unauthorized access to any part of your network? (If yes, explain on attached page.) [YES / NO]
36. Have you ever employed the services of a data recovery or computer forensic professional or company? (If yes, explain on attached page.) [YES / NO]
37. Would your computer systems remain operational if there was a loss of primary electrical power of more than two hours? [YES / NO]
38. Do you have personnel exclusively dedicated to computer security? [YES / NO]
39. Do you employ outside contractors to do any of the following:
   Network Administration [YES / NO]
   Web Programming [YES / NO]
   Database Administration [YES / NO]
   Firewall Administration [YES / NO]
   Intrusion Detection System Administration [YES / NO]
40. Security Administration for Security Patches, Hot Fixes, Improvements or Updates [YES / NO]
41. Network design, improvement or modification [YES / NO]
42. Do you monitor and escort visitors through critical parts of your company?  
43. Do you maintain visitor logs for more than 30 days?  
44. Have you ever suspected a visitor of any malicious computer activity?  
45. Do you have, or have you made plans to install, integrate or in any form connect any type of wireless networking access hardware or device upon your computer network or web farm? (If yes, explain on attached page.)  
46. Has a network security engineer, security professional, or other employee with access to critical components of your network (administrators, etc) ever been physically threatened, stalked or placed in fear for their personal safety? (If yes, explain on attached page.)  
47. Do you periodically check your network to ensure that no unauthorized equipment has been attached to your network?  
48. Have you ever discovered any unauthorized equipment on your network? (If yes, explain on attached page.)
A. Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Firewalls are computer devices that control computer traffic allowed into and out of a company’s network, as well as traffic into more sensitive areas within a company’s internal network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from the Internet, whether entering the system as e-commerce, employees’ Internet-based access through desktop browsers, or employees’ e-mail access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

Establish firewall configuration standards that include the following:

- A formal process for approving and testing all external network connections and changes to the firewall configuration
- A current network diagram with all connections to cardholder data, including any wireless networks
- Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone
- Description of groups, roles, and responsibilities for logical management of network components
- Documented list of services and ports necessary for business
• Justification and documentation for any available protocols besides hypertext transfer protocol (HTTP), and secure sockets layer (SSL), secure shell (SSH), and virtual private network (VPN)

• Justification and documentation for any risky protocols allowed (for example, file transfer protocol (FTP), which includes reason for use of protocol and security features implemented

• Quarterly review of firewall and router rule sets

• Configuration standards for routers.

Build a firewall configuration that denies all traffic from “untrusted” networks and hosts, except for protocols necessary for the cardholder data environment.

Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks. This firewall configuration should include the following:

• Restricting inbound Internet traffic to Internet protocol (IP) addresses within the DMZ (ingress filters)

• Not allowing internal addresses to pass from the Internet into the DMZ

• Implementing stateful inspection, also known as dynamic packet filtering (that is, only "established" connections are allowed into the network)

• Placing the database in an internal network zone, segregated from the DMZ

• Restricting inbound and outbound traffic to that which is necessary for the cardholder data environment

• Securing and synchronizing router configuration files. For example, running configuration files (for normal functioning of the routers), and start-up 1.3.7 configuration files (when machines are re-booted) should have the same secure configuration

• Denying all other inbound and outbound traffic not specifically allowed
Installing perimeter firewalls between any wireless networks and the cardholder data environment, and configuring these firewalls to deny any traffic from the wireless environment or from controlling any traffic (if such traffic is necessary for business purposes)

Installing personal firewall software on any mobile and employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.

Prohibit direct public access between external networks and any system component that stores cardholder data (for example, databases, logs, trace files).

- Implement a DMZ to filter and screen all traffic and to prohibit direct routes for inbound and outbound Internet traffic
- Restrict outbound traffic from payment card applications to IP addresses within the DMZ.
- Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet. Use technologies that implement RFC 1918 address space, such as port address translation (PAT) or network address translation (NAT).

**Requirement 2:** Do not use vendor-supplied defaults for system passwords and other security parameters

Hackers (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and easily determined via public information.

Always change vendor-supplied defaults before installing a system on the network (for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts).

For wireless environments, change wireless vendor defaults, including but not limited to, wired equivalent privacy (WEP) keys, default service set identifier (SSID), passwords, and SNMP community strings.
Disable SSID broadcasts. Enable WiFi protected access (WPA and WPA2) technology for encryption and authentication when WPA-capable.

Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards as defined, for example, by SysAdmin Audit Network Security Network (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS).

- Implement only one primary function per server (for example, web servers, database servers, and DNS should be implemented on separate servers)
- Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices’ specified function)
- Configure system security parameters to prevent misuse
- Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.

Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other non-console administrative access.

Hosting providers must protect each entity’s hosted environment and data. These providers must meet specific requirements as detailed in Appendix A: “PCI DSS Applicability for Hosting Providers”
B. Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Encryption is a critical component of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed and not sending PAN in unencrypted e-mails.

Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.

Do not store sensitive authentication data subsequent to authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:

Do not store the full contents of any track from the magnetic stripe (that is on the back of a card, in a chip or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data. In the normal course of business, the following data elements from the magnetic stripe may need to be retained: the account holder’s name, primary account number (PAN), expiration date, and service code. To minimize risk, store only those data elements needed for business. NEVER store the card verification code or value or PIN verification value data elements. Note: See “Glossary” for additional information.

Do not store the card-validation code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions. Note: See “Glossary” for additional information.

Do not store the personal identification number (PIN) or the encrypted PIN block.

Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed). Note: This requirement does
not apply to employees and other parties with a specific need to see the full PAN; nor does the requirement supersede stricter requirements in place for displays of cardholder data (for example, for point of sale [POS] receipts).

Render PAN, at minimum, unreadable anywhere it is stored (including data on portable digital media, backup media, in logs, and data received from or stored by wireless networks) by using any of the following approaches:

- Strong one-way hash functions (hashed indexes)
- Truncation
- Index tokens and pads (pads must be securely stored)

Strong cryptography with associated key management processes and procedures. The MINIMUM account information that must be rendered unreadable is the PAN. If for some reason, a company is unable to encrypt cardholder data, refer to Appendix VIII: “Compensating Controls for Encryption of Stored Data.”

If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local system or Active Directory accounts). Decryption keys must not be tied to user accounts.

- Protect encryption keys used for encryption of cardholder data against both disclosure and misuse.
- Restrict access to keys to the fewest number of custodians necessary
- Store keys securely in the fewest possible locations and forms.

Fully document and implement all key management processes and procedures for keys used for encryption of cardholder data, including the following:

- Generation of strong keys
- Secure key distribution
- Secure key storage
Periodic changing of keys, as deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically At least annually.

- Destruction of old keys
- Split knowledge and establishment of dual control of keys (so that it requires two or three people, each knowing only their part of the key, to reconstruct the whole key)
- Prevention of unauthorized substitution of keys
- Replacement of known or suspected compromised keys
- Revocation of old or invalid keys
- Requirement for key custodians to sign a form stating that they understand and accept their key-custodian responsibilities.

**Requirement 4:** Encrypt transmission of cardholder data across open, public networks.

Sensitive information must be encrypted during transmission over networks that are easy and common for a hacker to intercept, modify, and divert data while in transit.

Use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS are the Internet, WiFi (IEEE 802.11x), global system for mobile communications (GSM), and general packet radio service (GPRS).

For wireless networks transmitting cardholder data, encrypt the transmissions by using WiFi protected access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS. Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN. If WEP is used, do the following:

- Use with a minimum 104-bit encryption key and 24 bit-initialization value.
- Use ONLY in conjunction with WiFi protected access (WPA or WPA2) technology, VPN, or SSL/TLS
- Rotate shared WEP keys quarterly (or automatically if the technology permits)
- Rotate shared WEP keys whenever there are changes in personnel with access to keys
- Restrict access based on media access code (MAC) address.
- Never send unencrypted PANs by e-mail.
- C. Maintain a Vulnerability Management Program

**Requirement 5:** Use and regularly update anti-virus software or programs. Many vulnerabilities and malicious viruses enter the network via employees’ e-mail activities. Anti-virus software must be used on all systems commonly affected by viruses to protect systems from malicious software.

Deploy anti-virus software on all systems commonly affected by viruses (particularly personal computers and servers) Note: Systems commonly affected by viruses typically do not include UNIX-based operating systems or mainframes.

Ensure that anti-virus programs are capable of detecting, removing, and protecting against other forms of malicious software, including spyware and adware.

Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.

**Requirement 6:** Develop and maintain secure systems and applications. Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches. All systems must have the most recently released, appropriate software patches to protect against exploitation by employees, external hackers, and viruses. Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing
security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

- Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.
- Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update standards to address new vulnerability issues.
- Develop software applications based on industry best practices and incorporate information security throughout the software development life cycle.
- Testing of all security patches and system and software configuration changes before deployment
- Separate development, test, and production environments
- Separation of duties between development, test, and production environments
- Production data (live PANs) are not used for testing or development
- Removal of test data and accounts before production systems become active
- Removal of custom application accounts, usernames, and passwords before applications become active or are released to customers
- Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability.
- Follow change control procedures for all system and software configuration changes. The procedures must include the following:
  - Documentation of impact
  - Management sign-off by appropriate parties
  - Testing of operational functionality
  - Back-out procedures
Develop all web applications based on secure coding guidelines such as the Open Web Application Security Project guidelines. Review custom application code to identify coding vulnerabilities. Cover prevention of common coding vulnerabilities in software development processes, to include the following:

- Unvalidated input
- Broken access control (for example, malicious use of user IDs)
- Broken authentication and session management (use of account credentials and session cookies)
- Cross-site scripting (XSS) attacks
- Buffer overflows
- Injection flaws (for example, structured query language (SQL) injection)
- Improper error handling
- Insecure storage
- Denial of service
- Insecure configuration management

Ensure that all web-facing applications are protected against known attacks by applying either of the following methods:

- Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security
- Installing an application layer firewall in front of web-facing applications.

**Note:** This method is considered a best practice until June 30, 2008, after which it becomes a requirement. D. Implement Strong Access Control Measures
**Requirement 7:** Restrict access to cardholder data by business need-to-know.

- This requirement ensures critical data can only be accessed by authorized personnel.
- Limit access to computing resources and cardholder information only to those individuals whose job requires such access.
- Establish a mechanism for systems with multiple users that restricts access based on a user’s need to know and is set to “deny all” unless specifically allowed.

**Requirement 8:** Assign a unique ID to each person with computer access

Assigning a unique identification (ID) to each person with access ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

- Identify all users with a unique user name before allowing them to access system components or cardholder data.
- In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:
  - Password
  - Token devices (e.g., SecureID, certificates, or public key)
  - Biometrics.

Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.

- Encrypt all passwords during transmission and storage on all system components.
- Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:
- Control addition, deletion, and modification of user IDs, credentials, and other identifier objects
- Verify user identity before performing password resets
- Set first-time passwords to a unique value for each user and change immediately after the first use
- Immediately revoke access for any terminated users
- Remove inactive user accounts at least every 90 days
- Enable accounts used by vendors for remote maintenance only during the time period needed
- Communicate password procedures and policies to all users who have access to cardholder data
- Do not use group, shared, or generic accounts and passwords
- Change user passwords at least every 90 days
- Require a minimum password length of at least seven characters
- Use passwords containing both numeric and alphabetic characters
- Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used
- Limit repeated access attempts by locking out the user ID after not more than six attempts
- Set the lockout duration to thirty minutes or until administrator enables the user ID
- If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal
- Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users
**Requirement 9:** Restrict physical access to cardholder data.

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted.

- Use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data.
- Use cameras to monitor sensitive areas. Audit collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.
- Restrict physical access to publicly accessible network jacks.
- Restrict physical access to wireless access points, gateways, and handheld devices.

Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. “Employee” refers to full-time and part-time employees, temporary employees and personnel, and consultants who are “resident” on the entity’s site. A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the facility for a short duration, usually not more than one day.

Make sure all visitors are handled as follows:

- Authorized before entering areas where cardholder data is processed or maintained.
- Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as non-employees.
- Asked to surrender the physical token before leaving the facility or at the date of expiration.
- Use a visitor log to maintain a physical audit trail of visitor activity. Retain this log for a minimum of three months, unless otherwise restricted by law.
- Store media back-ups in a secure location, preferably in an off-site facility, such as an alternate or backup site, or a commercial storage facility.
Physically secure all paper and electronic media (including computers, electronic media, networking and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes) that contain cardholder data.

Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data including the following:

- Classify the media so it can be identified as confidential
- Send the media by secured courier or other delivery method that can be accurately tracked.
- Ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals).
- Maintain strict control over the storage and accessibility of media that contains cardholder data.
- Properly inventory all media and make sure it is securely stored.

Destroy media containing cardholder data when it is no longer needed for business or legal reasons as follows:

- Cross-cut shred, incinerate, or pulp hardcopy materials
- Purge, degauss, shred, or otherwise destroy electronic media so that cardholder data cannot be reconstructed.

E. Regularly Monitor and Test Networks

**Requirement 10:** Track and monitor all access to network resources and cardholder data.

Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis if something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

- Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.
- Implement automated audit trails for all system components to reconstruct the following events:
o All individual user accesses to cardholder data
o All actions taken by any individual with root or administrative privileges
o Access to all audit trails
o Invalid logical access attempts
o Use of identification and authentication mechanisms
o Initialization of the audit logs
o Creation and deletion of system-level objects.

- Record at least the following audit trail entries for all system components for each event:
  o User identification
  o Type of event
  o Date and time
  o Success or failure indication
  o Origination of event
  o Identity or name of affected data, system component, or resource.
  o Synchronize all critical system clocks and times.
  o Secure audit trails so they cannot be altered.
  o Limit viewing of audit trails to those with a job-related need
  o Protect audit trail files from unauthorized modifications
  o Promptly back-up audit trail files to a centralized log server or media that is difficult to alter
  o Copy logs for wireless networks onto a log server on the internal LAN.

Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).

Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). Note: Log harvesting, parsing and alerting tools may be used to achieve compliance with Requirement 10.6.
Retain audit trail history for at least one year, with a minimum of three months online availability.

**Requirement 11: Regularly test security systems and processes.** Vulnerabilities are being discovered continually by hackers and researchers, and being introduced by new software. Systems, processes, and custom software should be tested frequently to ensure security is maintained over time and with any changes in software.

Test security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts. Use a wireless analyzer at least quarterly to identify all wireless devices in use.

Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).

**Note:** Quarterly external vulnerability scans must be performed by a scan vendor qualified by the payment card industry. Scans conducted after network changes may be performed by the company’s internal staff.

Perform penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following:

- Network-layer penetration tests
- Application-layer penetration tests.

Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date.

Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files; and configure the software to perform critical file comparisons at least weekly. Critical
files are not necessarily only those containing cardholder data. For file integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is the merchant or service provider).

F. Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for employees and Contractors.

A strong security policy sets the security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it.

Establish, publish, maintain, and disseminate a security policy that accomplishes the following:

- Addresses all requirements in this specification
- Includes an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment
- Includes a review at least once a year and updates when the environment changes.

Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).

Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors. Ensure these usage policies require the following:

- Explicit management approval
- Authentication for use of the technology
- List of all such devices and personnel with access
- Labeling of devices with owner, contact information, and purpose
- Acceptable uses of the technologies
- Acceptable network locations for the technologies
- List of company-approved products
- Automatic disconnect of modem sessions after a specific period of inactivity
- Activation of modems for vendors only when needed by vendors, with immediate deactivation after use

When accessing cardholder data remotely via modem, prohibition of storage of cardholder data onto local hard drives, floppy disks, or other external media. Prohibition of cut-and-paste and print functions during remote access.

Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors.

Assign to an individual or team the following information security management responsibilities:
- Establish, document, and distribute security policies and procedures
- Monitor and analyze security alerts and information, and distribute to appropriate personnel
- Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations
- Administer user accounts, including additions, deletions, and modifications
- Monitor and control all access to data.
- Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.
- Educate employees upon hire and at least annually (for example, by letters, posters, memos, meetings, and promotions)
- Require employees to acknowledge in writing that they have read and understood the company’s security policy and procedures.
- Screen potential employees to minimize the risk of attacks from internal sources.
• For those employees such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.

If cardholder data is shared with service providers, then contractually the following is required:
• Service providers must adhere to the PCI DSS requirements
• Agreement that includes an acknowledgement that the service provider is responsible for the security of cardholder data the provider possesses.
• Implement an incident response plan. Be prepared to respond immediately to a system breach.

Create the incident response plan to be implemented in the event of system compromise. Ensure the plan addresses, at a minimum, specific incident response procedures, business recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies (for example, informing the Acquirers and credit card associations)
• Test the plan at least annually
• Designate specific personnel to be available on a 24/7 basis to respond to alerts
• Provide appropriate training to staff with security breach response responsibilities
• Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems
• Develop process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.

All processors and service providers must maintain and implement policies and procedures to manage connected entities, to include the following:
- Maintain a list of connected entities
- Ensure proper due diligence is conducted prior to connecting an entity
- Ensure the entity is PCI DSS compliant
- Connect and disconnect entities by following an established process.
## APPENDIX –X

### MERCHANT LEVELS AND VALIDATION REQUIREMENTS

<table>
<thead>
<tr>
<th>Level</th>
<th>Visa</th>
<th>MasterCard</th>
<th>JCB</th>
<th>American Express</th>
<th>Discover</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Any merchant processing over 6,000,000 Visa transactions per year OR any merchant that Visa determines should meet the Level 1 merchant requirements to minimize risk to the Visa system.</td>
<td>Merchants processing over 6 million MasterCard transactions annually, identified by another payment card brand as Level 1</td>
<td>Merchants processing over 1 million JCB transactions annually, or compromised merchants</td>
<td>Merchants processing over 2.5 million American Express Card transactions annually or any merchant that American Express deems a Level 1</td>
<td>Merchants are currently not categorized into levels based on transaction volume. Discover takes a &quot;risk based approach&quot; for validating compliance</td>
</tr>
<tr>
<td>2.</td>
<td>Any merchant processing 1,000,000 to 6,000,000 Visa transactions per year</td>
<td>Merchants processing 1 million to 6 million MasterCard transactions annually</td>
<td>Merchants processing less than 1 million JCB transactions annually</td>
<td>Merchants providing 50,000 to 2.5 million American Express transactions annually or any merchant that American Express deems Level 2</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Any merchant processing 20,000 to 1,000,000 Visa e-commerce transactions per year</td>
<td>Merchants processing 20,000 to 1 million MasterCard e-commerce transactions annually</td>
<td>N/A</td>
<td>Merchants processing less than 50,000 American Express transactions annually</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants-regardless of acceptance channel-</td>
<td>All other MasterCard Merchants</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Sl. No.</td>
<td>Merchant Validation Requirements</td>
<td>American Express</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Annual onsite review by QSA (PCI DSS Assessment) and Quarterly Network Scan by ASV</td>
<td>Annual onsite review by QSA (PCI DSS Assessment) and Quarterly Network Scan by ASV</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td></td>
<td>Quarterly Network Scan by ASV AND one of the following: Annual onsite review by QSA- PCI DSS Assessment and Annual Self Assessment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Annual Self Assessment Questionnaire and Quarterly Network Scan by ASV</td>
<td>Quarterly Network Scan by ASV</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Quarterly Network Scan by ASV AND one of the following: Annual onsite review by QSA- PCI DSS Assessment and Annual Self Assessment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Annual Self Assessment Questionnaire and Quarterly Network Scan by ASV</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Annual SAQ recommended Quarterly network scan by ASV if applicable Compliance validation requirements set by acquirer</td>
<td>Annual Self Assessment Questionnaire Quarterly Network Scan by ASV</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Quarterly Network Scan by ASV</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## APPENDIX XI

**PCI and ISO/IEC 27001 Relationship Matrix**

**PCI and ISO/IEC 27001 Mapping**

<table>
<thead>
<tr>
<th>PCI DSS</th>
<th>ISO/IEC 27001 CONTROLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Install &amp; Maintain Firewall</td>
<td></td>
</tr>
<tr>
<td>2. Do not use vendor supplied</td>
<td></td>
</tr>
<tr>
<td>3. Protect stored</td>
<td></td>
</tr>
<tr>
<td>4. Encrypt transmission of cardholder</td>
<td></td>
</tr>
<tr>
<td>5. Use and regularly</td>
<td></td>
</tr>
<tr>
<td>6. Develop and maintain secure</td>
<td></td>
</tr>
<tr>
<td>7. Restrict access to cardholder</td>
<td></td>
</tr>
<tr>
<td>8. Assign a unique ID to each person</td>
<td></td>
</tr>
<tr>
<td>9. Restrict physical access to</td>
<td></td>
</tr>
</tbody>
</table>
10. Track and monitor all access to network
11. Regularly test security
12. Maintain a policy that

The following elements from the PCI DSS Requirements are addressed in the ISO/IEC 27001:

A.5: Security Policy
- Information Security Policy Document
- Review of the Information Security Policy

A.6: Organization of Information Security
- Addressing security in third party agreements
- Allocation of information security responsibilities
- Confidentiality agreement
- Contact with special interest groups
- Information Security coordination

A.7: Asset Management
- Acceptable use of assets
- Information of removable media
- Inventory of Assets
- Ownership of Assets

A.8: Human Resources Security
- Information security awareness, education, and training
- Removal of access rights
- Roles and responsibilities
- Screening
- Terms and conditions of employment
A.9: Physical and Environmental Security

- Cabling Security
- Equipment protection
- Physical entry controls
- Physical security perimeter
- Protecting against external and environmental threats
- Securing offices, rooms, and facilities

A.10: Communications and Operations Management

- Audit Logging
- Change control procedure
- Change Management
- Clock Synchronization
- Disposal of media
- Documented Operating Procedures
- Electronic messaging
- Fault Logging
- Information Backup
- Information exchange policies and procedure
- Management of removable media
- Managing changes to third party services
- Monitoring system use
- Monitoring
- Network Controls
- Network Security Management
- Physical media in transit
- Protection against malicious and mobile code
- Protection of log information
- Segregation of duties
- Separation of development, test and operational facilities
- Third Party Service Management
A.11: Access Control

- Access Control Policy
- Access Management
- Application and information access control
- Business Requirement for access control
- Clear desk and clear screen policy
- Equipment identification in networks
- Network Access Control
- Network Connection Control
- Network routing control
- Password Management System
- Password use
- Policy on the use of Network Services
- Privilege Management
- Remote diagnostic and configuration port protection
- Secure log-on procedures
- Segregation in Networks
- Sensitive system isolation
- Session Time out
- Teleworking
- Use of system utilities
- User Access Management
- User authentication for external connections
- User identification and authentication
- User password Management
- User Registration

A.12: Information Systems Acquisition, Development and Maintenance

- Change control procedure
- Control of internal processing
- Control of operational software
- Control of technical vulnerabilities
- Information Leakage
• Input data validation
• Key management
• Policy on the use of cryptographic controls
• Restrictions on changes to software packages
• Security requirements analysis and specification
• Technical review of applications after operating system changes

A.13: Information Security Incident Management
• Information Security Incident Management

A.14: Business Continuity Management
• Business Continuity and Risk Assessment
• Business Continuity Management

A.15: Compliance
• Compliance with security policies and standards
<table>
<thead>
<tr>
<th>Section 1.0</th>
<th>PCI DSS 1.1 (Effective January 7, 2007)</th>
<th>PCI DSS 1.0 (Released September 5, 2006)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.8</td>
<td>Quarterly review of firewall and router rule sets removed</td>
<td>Period review of firewall/router rule sets</td>
</tr>
<tr>
<td></td>
<td>1.3.2 Restricting inbound and outbound Internet traffic to ports 80 and 443</td>
<td>1.4 Prohibit direct public access between external networks and any system component that stores cardholder data (for example, databases)</td>
</tr>
<tr>
<td></td>
<td>1.3.2 Restricting inbound and outbound Internet traffic to ports 80 and 443</td>
<td>1.4 Prohibit direct public access between external networks and any system component that stores cardholder data (for example, databases)</td>
</tr>
<tr>
<td>Section 2.0</td>
<td>2.1.1 For wireless environments, change wireless vendor defaults, including but not limited to, wireless equivalent privacy (WEP) keys, default service set identifier (SSID), passwords, and SNMP community strings. Disable SSID broadcasts. Enable WiFi protected access (WPA and WPA2) technology for encryption and authentication when WPA-capable.</td>
<td>2.1.1 For wireless environments, change wireless vendor defaults, including but not limited to, wireless equivalent privacy (WEP) keys, default service set identifier (SSID), passwords, and SNMP community strings. Disable SSID broadcasts. Enable WiFi protected access (WPA) technology for encryption and authentication when WPA-capable.</td>
</tr>
<tr>
<td></td>
<td>2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards as defined, for example, by SysAdmin Audit Network Security</td>
<td>2.2 Develop configuration standards for all system components. Make sure these standards address all known security vulnerabilities and are consistent with industry best practices.</td>
</tr>
</tbody>
</table>
2.4 Hosting providers must protect each entity’s hosted environment and data. These providers must meet specific requirements as detailed in Appendix A: “PCI DSS Applicability for Hosting Providers.”

| Section 3.0 | 3.4 Render PAN, at minimum, unreadable anywhere it is stored (including data on portable digital media, backup media, in logs, and data received from or stored by wireless networks) by using any of the following approaches:
|             | Strong one-way hash functions (hashed indexes)
|             | Truncation
|             | Index tokens and pads (pads must be securely stored)
|             | Strong cryptography with associated key management processes and procedures.
|             | The MINIMUM account information that must be rendered unreadable is the PAN.
|             | If for some reason, a company is unable to encrypt cardholder data, refer to Appendix B: “Compensating Controls for Encryption of Stored Data.”

| 3.4 Render sensitive cardholder data unreadable anywhere it is stored (including data on portable digital media, backup media, in logs, and data received from or stored by wireless networks) by using any of the following approaches:
| One-way hashes (hashed indexes), such as SHA-1
| Truncation
| Index tokens and PADs, with the PADs being securely stored
| Strong cryptography, such as Triple-DES (Data Encryption Standard) 128-bit or AES 256-bit
| with associated key management processes and procedures.
| The minimum account information that needs to be rendered unreadable is the payment card account number.
<table>
<thead>
<tr>
<th>Section</th>
<th>PCI DSS 1.1 (Effective January 7, 2007)</th>
<th>PCI DSS 1.0 (Released September 5, 2006)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.4.1</td>
<td>If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local system or Active Directory accounts). Decryption keys must not be tied to user accounts.</td>
<td>N/A</td>
</tr>
<tr>
<td>3.6.4</td>
<td>Periodic changing of keys As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically At least annually.</td>
<td>3.6.4 Periodic key changes.</td>
</tr>
<tr>
<td>4.0</td>
<td>4.1 Use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS are the Internet, WiFi (IEEE 802.11x), global system for mobile communications (GSM), and general packet radio service (GPRS).</td>
<td>4.1 Use strong cryptography and encryption techniques (at least 128 bit) such as SSL, Point-to-Point Tunneling Protocol (PPTP), Internet Protocol Security (IPSEC) to safeguard sensitive cardholder data during transmission over public networks.</td>
</tr>
<tr>
<td>4.1</td>
<td>4.1.1 For wireless networks transmitting cardholder data, encrypt the transmissions by using WiFi</td>
<td>4.1.1 For wireless networks transmitting cardholder data, encrypt the transmissions by using WiFi</td>
</tr>
</tbody>
</table>
protected access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS. Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN. If WEP is used, do the following:

- Use with a minimum 104-bit encryption key and 24 bit initialization value
- Use ONLY in conjunction with WiFi protected access (WPA or WPA2) technology, VPN, or SSL/TLS
- Rotate shared WEP keys quarterly (or automatically if the technology permits)
- Rotate shared WEP keys whenever there are changes in personnel with access to keys
- Restrict access based on media access code (MAC) address.

Wi-Fi Protected Access (WPA) technology if WPA capable, or VPN or SSL at 128-bit. Never rely exclusively on WEP to protect confidentiality and access to a wireless Local Area Network (LAN). Use one of the above methodologies in conjunction with WEP at 128 bit, and rotate shared WEP keys quarterly and whenever there are personnel changes.

<table>
<thead>
<tr>
<th>4.2 Never send unencrypted PANs by e-mail</th>
<th>5.0 Deploy anti-virus software on all systems commonly affected by viruses (particularly personal computers and servers)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Section</strong> 5.0</td>
<td>Note: Systems commonly affected by viruses typically do not include UNIX-based operating systems or mainframes.</td>
</tr>
<tr>
<td>Never send cardholder information via unencrypted email</td>
<td>Deploy anti-virus mechanisms on all systems commonly affected by viruses (for example PC’s and servers).</td>
</tr>
</tbody>
</table>
## Payment Card Industry Data Security Standard 1.1/1.0 Comparison

<table>
<thead>
<tr>
<th>Section</th>
<th>PCI DSS 1.1 (Effective January 7, 2007)</th>
<th>PCI DSS 1.0 (Released September 5, 2006)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1.1</td>
<td>5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against other forms of malicious software, including spyware and adware.</td>
<td>N/A</td>
</tr>
<tr>
<td>6.6</td>
<td>6.6 Ensure that all web-facing applications are protected against known attacks by applying either of the following methods: Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security Installing an application layer firewall in front of web-facing applications. Note: This method is considered a best practice until June 30, 2008, after which it becomes a requirement.</td>
<td>N/A</td>
</tr>
<tr>
<td>9.5</td>
<td>9.5 Store media back-ups in a secure location, preferably in an off-site facility, such as an alternate or backup site, or a commercial storage facility.</td>
<td>9.5 Store media back-ups in a secure off-site facility, which may be either an alternate third-party or a commercial storage facility.</td>
</tr>
<tr>
<td>10.5.5</td>
<td>10.5.5 Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts</td>
<td>10.5.5 Use file integrity monitoring/change detection software (such as Tripwire) on logs to ensure that existing log data cannot be changed without generating alerts</td>
</tr>
</tbody>
</table>
(although new data being added should not cause an alert).

<table>
<thead>
<tr>
<th>10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). Note: Log harvesting, parsing, and alerting tools may be used to achieve compliance with Requirement 10.6.</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.6 Review logs for all system components at least daily. Log reviews should include those servers that perform security functions like Intrusion Detection System (IDS) and Authentication, Authorization, and Accounting (AAA) servers (for example, RADIUS).</td>
</tr>
</tbody>
</table>

| Section 11 | 11.3 Perform penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following: 11.3.1 Network-layer penetration tests 11.3.2 Application-layer penetration tests. |
| Section 11 | 11.3 Perform penetration testing on network infrastructure and applications at least once a year and after any significant infrastructure or application upgrade or modification (for example, operating system upgrade, sub-network added to environment, Web server added to environment). |

### Payment Card Industry Data Security Standard 1.1/1.0 Comparison

<p>| Section 12 | PCI DSS 1.1 (Effective January 7, 2007) 12.6 Implement a formal security awareness program to make all employees aware of the importance of cardholder protections. |
| Section 12 | PCI DSS 1.0 (Released September 5, 2006) 12.6 Make all employees aware of the importance of cardholder protections. |</p>
<table>
<thead>
<tr>
<th>employees aware of the importance of cardholder data security. Educate employees upon hire and at least annually (for example, by letters, posters, memos, meetings, and promotions). Require employees to acknowledge in writing that they have read and understood the company’s security policy and procedures.</th>
<th>information security. Educate employees (for example, through posters, letters, memos, meetings, and promotions). Require employees to acknowledge in writing that they have read and understood the company’s security policy and procedures.</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.8 If cardholder data is shared with service providers, then contractually the following is required. Service providers must adhere to the PCI DSS requirements. Agreement that includes an acknowledgement that the service provider is responsible for the security of cardholder data the provider possesses.</td>
<td>12.8 Contractually require all third parties with access to cardholder data to adhere to payment card industry security requirements. At a minimum, the agreement should address: 12.8.1 Acknowledgement that the 3rd party is responsible for security of cardholder data in their possession. 12.8.2 Ownership by each Payment Card brand, Acquirer, and Merchants of cardholder data and acknowledgement that such data can ONLY be used for assisting these parties in completing a transaction, supporting a loyalty program, providing fraud control services, or for others uses specifically required by law. 12.8.3 Business continuity in the event of a major disruption, disaster, or failure. 12.8.4 Audit provisions that</td>
</tr>
<tr>
<td>12.10 All processors and service providers must maintain and implement policies and procedures manage connected entities, to include the following: Maintain a list of connected entities. Ensure proper due diligence is conducted prior to connecting an entity. Ensure the entity is PCI DSS compliant. 12.10.4 Connect and disconnect entities by following an established process.</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### APPENDIX – XIII

**STATISTICAL ANALYSIS OF USER SURVEY OF CREDIT/DEBIT CARD HOLDERS**

<table>
<thead>
<tr>
<th></th>
<th>Sex</th>
<th>Age</th>
<th>Qualification</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Female</td>
<td>Male</td>
<td>15-25</td>
<td>26-40</td>
</tr>
<tr>
<td>1.</td>
<td>Do you have credit card</td>
<td>16%</td>
<td>31%</td>
<td>4%</td>
</tr>
<tr>
<td>2.</td>
<td>Do you have debit card</td>
<td>61%</td>
<td>68%</td>
<td>50%</td>
</tr>
<tr>
<td>3.</td>
<td>Do you think your personal data protected by banks</td>
<td>73%</td>
<td>88%</td>
<td>74%</td>
</tr>
<tr>
<td>4.</td>
<td>Do you foresee any fraud in bank transaction</td>
<td>57%</td>
<td>51%</td>
<td>26%</td>
</tr>
<tr>
<td>5.</td>
<td>Do you use ATM without any technical problem?</td>
<td>50%</td>
<td>65%</td>
<td>50%</td>
</tr>
<tr>
<td>6.</td>
<td>Do you find difficulty in remembering PIN of your card?</td>
<td>31%</td>
<td>16%</td>
<td>35%</td>
</tr>
<tr>
<td></td>
<td>Question</td>
<td>90%</td>
<td>91%</td>
<td>89%</td>
</tr>
<tr>
<td>---</td>
<td>--------------------------------------------------------------------------</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>7.</td>
<td>Do you feel the ATM useful in withdrawing money?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td>Do you ever faced difficulty in using ATM</td>
<td>82%</td>
<td>77%</td>
<td>32%</td>
</tr>
<tr>
<td>9.</td>
<td>Do you feel credit/debit card number in secured</td>
<td>50%</td>
<td>69%</td>
<td>54%</td>
</tr>
<tr>
<td>10.</td>
<td>Do you find Master/Visa/Maestro logo on your card</td>
<td>51%</td>
<td>66%</td>
<td>60%</td>
</tr>
<tr>
<td>11.</td>
<td>Do you find debit/credit card is secured while using online purchase?</td>
<td>32%</td>
<td>42%</td>
<td>35%</td>
</tr>
<tr>
<td>12.</td>
<td>Do you feel cards are safe to use in petrol bunk and super bazaar</td>
<td>36%</td>
<td>36%</td>
<td>31%</td>
</tr>
<tr>
<td>13.</td>
<td>Do you think banks are well prepaed to take your complaint regarding credit/debit card</td>
<td>49%</td>
<td>66%</td>
<td>65%</td>
</tr>
<tr>
<td></td>
<td>Question</td>
<td>48%</td>
<td>57%</td>
<td>64%</td>
</tr>
<tr>
<td>---</td>
<td>--------------------------------------------------------------------------</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>14.</td>
<td>Do you think RBI guidelines are strictly followed by banks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15.</td>
<td>Do you think bank managers are well educated to address your credit/debit problems</td>
<td>50%</td>
<td>64%</td>
<td>59%</td>
</tr>
<tr>
<td>16.</td>
<td>Do you think purchasing through online safe and secured</td>
<td>20%</td>
<td>25%</td>
<td>27%</td>
</tr>
<tr>
<td>17.</td>
<td>Do you think banks are transparent in their transactions?</td>
<td>46%</td>
<td>60%</td>
<td>69%</td>
</tr>
<tr>
<td>18.</td>
<td>Do you think Nationalized banks are giving good services.</td>
<td>73%</td>
<td>76%</td>
<td>70%</td>
</tr>
<tr>
<td>19.</td>
<td>Do you feel cyber frauds has increased after E-banking</td>
<td>70%</td>
<td>72%</td>
<td>86%</td>
</tr>
<tr>
<td>20.</td>
<td>Do you feel RBI has to control over foreign banks</td>
<td>51%</td>
<td>56%</td>
<td>46%</td>
</tr>
</tbody>
</table>