SERVICE AGREEMENT
FOR THE RSA FRAUD ACTION SERVICES

THIS SERVICE AGREEMENT FOR THE RSA FRAUD ACTION SERVICES ("**AGREEMENT**") IS EFFECTIVE AS OF THE DATE OF THE CUSTOMER'S SIGNED ACCEPTANCE OF THE APPLICABLE QUOTATION MAKING REFERENCE TO THIS AGREEMENT.

ANY AND ALL REFERENCES TO "**CUSTOMER**" SHALL BE DEEMED TO MEAN THE CUSTOMER SET FORTH IN AN APPLICABLE QUOTATION.

If Customer is located in the United States, Mexico or South America, then this is a legal agreement between the Customer and RSA with "**RSA**" meaning RSA Security LLC.

If Customer is located outside of the United States, Mexico or South America, then this is a legal agreement between the Customer and RSA, with "RSA" meaning (i) the local EMC sales subsidiary, if Customer is located in a country in which RSA does business through a local EMC Corporation sales subsidiary; or (ii) EMC Information Systems International ("EISI"), if Customer is located in a country in which EMC Corporation does not have a local sales subsidiary).

THIS AGREEMENT SETS FORTH THE GENERAL TERMS AND CONDITIONS UNDER WHICH RSA WILL PROVIDE AND CUSTOMER WILL RECEIVE THE FRAUD ACTION SERVICES ("**FAS**") (AS DEFINED BELOW).

1. DEFINITIONS. The following terms shall have the definitions below or set forth elsewhere herein.

"**APS Incident**" means: (a) either of one (1) Universal Resource Locator (herein a "URL"); one (1) internet domain; or one (1) website; which direct account holders and/or clients of the Customer to those specific web based locations; or (b) one (1) email account associated with either of the above web based locations and which is used for the collection of compromised credentials (including e-mail mailbox involved in advance fee fraud "419" e-mail scams); and with respect to which RSA took action to close down or block the web based location or email account; used counter-measures; or performed forensic work (in all cases as described in Exhibit A);

"**ATS Incident**" means in relation to the ATS: one (1) element of Crimeware, uniquely identified using the "MD5 hash" method via what is commonly known as the Universally Unique Identifier ("UUID"), with respect to which RSA took action to detect and analyze a Trojan, perform forensic work, close down or block the domain or IP address of the "Infection Point", (the site which executes a code routine for the purpose of installing or updating Crimeware with or without the consent of the website viewer or which makes Crimeware available for download by third parties)or, a "Command and Control" point (being a computer which receives information from or controls a Trojan installed on a third party's computer), or an "Update Point" (an web based resource from which Crimeware may download software updates or new configuration instructions), or "Drop Site" (including an email account which is used for the collection of compromised credentials) in all cases as described in Exhibit A;

"**Crimeware**" means software or other software applications or executables designed to misappropriate personal credentials, personal data and/or to engage in fraudulent transactions using improperly obtained identity information, all for the purpose of assisting with or performing illegal or improper acts;

"**Customer Domain**" means one (1) unique trademark, trade name, word mark, service mark or other designation for which the Customer claims ownership or rights thereto;

"**Documentation**" means the manuals, handbooks and/or other information outlining the functionality of the FAS whether in hard copy or soft copy form, that RSA may provide with the FAS;

"**eFraudNetwork**" database means a database operated by RSA which contains information aggregated by RSA, discovered by the Parties as part of the performance of their obligations under this Agreement, obtained, and/or procured from third Parties and/or resulting from risk and fraud assessments carried out by RSA. For the avoidance of doubt, the eFraudNetwork[SM] database does not include any Confidential Information of the Parties or any Non Public Personal Information as defined in Section 7 below;

"**Exhibit**" means Exhibit A attached hereto, the terms of which are incorporated herein by reference;

"**Fraud Action Service**" ("**FAS**")" shall mean any of RSA's services for addressing certain methods of online fraud which are offered to Customer as a managed service under this Agreement which include jointly or separately the "Anti-Phishing Service", the "Anti-Pharming Service" and/or the "Anti-Trojan Service" as further detailed in Exhibit A. The FAS shall also include without limitation: any and all Intellectual Property pertaining thereto and the Documentation;

"**Incident**" means either of an APS Incident or an ATS Incident;

"**Information**" means any information discovered by RSA in the performance of the FAS and communicated to Customer, including but not limited to information which may appear to indicate specific, ongoing or planned fraudulent exploits and vulnerabilities which relate to or may affect the business of the Customer;

"**Quote**(**s**)" means one or more documents issued by RSA specifying the FAS that Customer seeks to obtain from RSA, the related pricing and sufficient other information to complete the transaction. The Quote shall incorporate this Agreement by reference;

"**Service Fee**" means the service fee stated in the mutually executed Quote for the FAS;

"**Territory**" means each country designated in Exhibit A where the Customer provides services to its account holders and other clients.

2. SERVICES.

a. So long as the Customer is current on the payment of any and all applicable amounts due to RSA hereunder, RSA will provide the FAS to Customer, for the term of Agreement, on a non-exclusive and non-transferable basis in order to detect certain forms of online fraud directed at Customer client accounts located in the Territory FAS (the "**Service**").

b. RSA shall implement and activate the FAS in accordance with the service setup form that the Parties shall use their reasonable endeavors to complete within seven (7) days from the Customer's acceptance of the Quotation ('**Service Setup Form**").

c. In consideration of the FAS rendered under this Agreement, Customer shall pay RSA the Service Fee together with any other fees and expenses as set forth in the applicable mutually signed RSA Quote. Customer shall reimburse RSA for travel and other usual and customary expenses incurred by RSA's personnel in connection with this Agreement.

3. TERM & TERMINATION.

a. This Agreement shall commence and become effective from the Customer's signed acceptance of the Quotation and shall remain in effect for a period specified in the Quotation counted from the date the FAS is first activated (the "**Activation Date**") (the "**Initial Term**"). Following the Initial Term, the Agreement will be renewed for subsequent twelve (12) month terms (each a "**Renewal Term**"), unless not less than sixty (60) days prior to the end of the Initial Term (or any subsequent Renewal Term), either Party indicates in writing to the other its intention not to renew this Agreement.

b. Either party may notify the other in writing in case of the other's alleged breach of a material provision of this Agreement. The recipient shall have thirty (30) days from the date of receipt of such notice to effect a cure. If the recipient of the notice fails to effect a cure within such period, then the sender of the notice shall have the option of sending a written notice of termination of the Agreement, which notice shall take effect upon receipt.

c. Upon termination of the Agreement, Customer shall promptly return to RSA, or destroy and certify in writing to RSA, that it has destroyed the original and all copies, in whole or in part, in any form, of the Documentation, and any other Confidential Information disclosed by RSA under the Agreement. Termination of the Agreement shall not discharge any payment obligations accrued as of the effective date of such termination even if such obligations are payable after the termination date. Upon any termination of this Agreement, Sections 3, 4, 5, 6, and 8 through 12 hereof shall survive in accordance with their terms.

4. OWNERSHIP, INTELLECTUAL PROPERTY RIGHTS AND LICENSE.

a. RSA shall retain and own all right, title and interest and all Intellectual Property in and to the Services and nothing herein transfers or conveys to the Customer any ownership right, title or interest in or to the Service or any license right with respect to same not expressly granted herein. As used herein, "**Intellectual Property**" shall include, without limitation, copyrights, trade-secrets, service names, trademarks (including the RSA Marks), trade-names, domain names, patents, know-how, formulation, data, technology, designs, inventions, improvements, discoveries, processes, models or sales, financial, contractual and marketing information and all other intellectual or industrial property and like rights whether or not registered and the applications thereof;

b. Subject to the terms and conditions of this Agreement, RSA grants Customer a non-exclusive, non-transferable, non-sub-licensable right to access and use the Services for the purpose for which it is made available to Customer in accordance with the Documentation.

c. Customer acknowledges that in providing the Services, RSA may utilize (i) the RSA name, the RSA logo, the RSA domain name, the product names associated with the Services and other trademarks; (ii) certain methodology, information, documents, software and other works of authorship; and (iii) other technology, software, hardware, products, processes, algorithms, user interfaces, know-how and other trade secrets, techniques, designs, inventions, look and feel of the Services and other tangible or intangible technical material or information (collectively "RSA Technology") and that the RSA Technology is the exclusive property of RSA, contains valuable trade secrets and Confidential Information of RSA, and is covered by Intellectual Property rights owned or licensed by RSA. Other than as expressly set forth in this Agreement, no license or other rights in the RSA Technology or the Services are granted to Customer, and all such rights are hereby expressly reserved. Nothing contained in this Agreement shall be deemed to convey to Customer any right, title or interest in or to the Services or data therein or the RSA Technology, except to the extent of the limited license granted in this Agreement.

d. Customer shall not (i) modify, copy or make derivative works based on the RSA Technology or the Services; (ii) disassemble, reverse engineer, or decompile any of the RSA Technology; or (iii) sell, sublicense, transfer or make available the RSA Technology or the Services to any third parties.

e. RSA shall retain and own all right, title and interest and all Intellectual Property Rights to all information which is collected, submitted to and made available on the eFraudNetwork database in the course of the performance

by either Party of their obligations under this Agreement (or where such title cannot be granted or otherwise transferred to RSA then Customer agrees to grant RSA an non-exclusive, fully paid and perpetual right to use, distribute and/or otherwise make available such information).

f. During the term of the Agreement, the Customer hereby grants to RSA, subject to the terms and conditions of this Agreement, a limited, royalty-free, non-exclusive, non-transferable, non sublicensable, worldwide right and license to use and display the Customer's trade names, trademarks, service marks and associated logos and other promotional materials set forth in the Service Setup Form (the "**Marks**"), solely to the extent necessary for RSA to perform its obligations hereunder, including but not limited to issuance of the cease and desist notice(s).

g. The Customer will retain all right, title and interest in and to its Marks, and all goodwill associated with use of such Marks will inure solely to the benefit of the Customer. All use of the Customer's Marks by RSA shall conform to good trademark usage practice or any reasonable trademark usage guidelines or instructions that the Customer may provide to RSA from time to time. No licenses are hereby granted by Customer to RSA with respect to the Marks except for those expressly set forth in this Agreement.

5. CONFIDENTIALITY.

a. **"Confidential Information"** means the terms of this Agreement and all confidential and proprietary information of RSA or Customer, including without limitation all business plans, product plans, financial information, software, designs, formulas, methods, know how, processes, materials provided to Customer in the course of performing Services under this Agreement**,** and technical, business and financial data of any nature whatsoever (including, without limitation, any marketing, pricing and other information regarding the Services), provided that such information is marked or designated in writing as "confidential," "proprietary," or any other similar term or designation. Confidential Information does not include information that is (i) rightfully in the receiving party's possession without obligation of confidentiality prior to receipt from the disclosing party; (ii) a matter of public knowledge through no fault of the receiving party; (iii) rightfully furnished to the receiving party by a third party without restriction on disclosure or use; or (iv) independently developed by the receiving party without use of or reference to the disclosing party's Confidential Information. Each party shall (i) use Confidential Information of the other party only for the purposes of exercising rights or performing obligations in connection with this Agreement , and (ii) use at least reasonable care to protect from disclosure to any third parties any Confidential Information disclosed by the other party for a period from the date hereof until three (3) years following the later of (i) the termination date of this Agreement or (ii) the last date of the completion or other termination of Services under this Agreement entered into hereunder, provided, however, that Confidential Information that constitutes, contains or reveals, in whole or in part, RSA proprietary rights shall not be disclosed by the receiving party at any time. Notwithstanding the foregoing, a receiving party may disclose Confidential Information pursuant to a valid order of a court or authorized government agency provided that the receiving party has given the disclosing party prompt notice, to the extent legally permissible, so that the disclosing party will have an opportunity to defend, limit or protect against such disclosure.

b. RSA may identify Customer for reference purposes unless and until Customer expressly objects in writing.

c. Customer may not disclose the results of any performance tests of a Service to any third party without RSA's prior written approval. Notwithstanding the foregoing, (i) RSA may disclose Customer Confidential Information to an Affiliate or contractor (who is under an obligation of confidentiality) for the purpose of fulfilling RSA's obligations or exercising RSA's rights hereunder so long as RSA and its Affiliates comply with the confidentiality obligations above.

d. The Parties do not intend to disclose to one another hereunder information that would be covered by the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act of 1996 or similar privacy legislation within or outside of the United States. Accordingly, neither Party shall disclose to the other hereunder any of the following information regarding either Party's employees, customers, suppliers or other business partners: protected health information (as defined at 45 CFR 164.501), social security numbers, driver's license numbers, credit card numbers or similar government identity numbers or personal financial account numbers (herein "Non Public Personal Information").

6. INVOICING & PAYMENT. A "FAS Service Year" means a calendar year counted from the Activation Date. The Service Fee is invoiced annually in advance from the FAS Activation Date and on each anniversary thereof (if renewed). If Service Fees are to be invoiced on a monthly basis, the monthly service fees are determined based on the total Annual Incident Allocation and are expressed on a monthly basis. Therefore, where Customer has exhausted its Incident Allocation before the expiration of the then current FAS Service Year, the stated monthly Service Fees will remain due and payable for the remainder of that FAS Service Year. All Incident counts and related payments are made on a FAS Service Year basis. If Customer exhausts the Incident Allocation before the end of the FAS Service Year, RSA shall suspend performance of the FAS until such time when Customer purchases additional Incidents pursuant to an additional RSA Quotation. All Incidents Allocated to a FAS Service Year must be used within that FAS Service Year; all unused Incidents shall expire without notice from RSA. Expired Incidents shall not be carried forward to any subsequent FAS Service Year. RSA shall submit invoices for fees and reimbursable costs and expenses and Customer shall pay each invoice in the manner specified herein. Customer will also pay all related taxes and withholdings, except for those based on RSA's net income. If Customer is required to withhold taxes, then Customer will forward any withholding receipts to RSA. Subject to RSA's credit approval, all amounts are due in the

currency stated on the invoice and in full 30 days after the date of RSA's invoice, with interest accruing thereafter at the lesser of 1.5% per month or the highest lawful rate.

7. WARRANTY.

a. RSA shall perform the Service (i) in a workmanlike manner and in accordance with generally accepted industry standards and (ii) substantially in accordance with the Documentation for such Service. Customer must notify RSA of any failure to so perform within ten (10) days after the date on which such failure first occurs. If RSA is unable to correct and/or re-perform the Service within a reasonable time, then RSA's entire liability and Customer's exclusive remedy for failure to so perform shall be at Customer's sole option and upon written notice to RSA, termination of the Agreement forthwith and RSA shall refund the remainder of any unused fees paid in advance by Customer for the affected Service and which remain undelivered as of the termination date.

b. Customer represents and warrants that:
   i. it has the authority and that it has obtained all necessary approvals in order to deliver private and/or personal data to RSA or its agents, if such data is delivered under this Agreement.
   ii. the information provided in the Service Setup Form (or any updates thereto provided by Customer from time to time) is complete and accurate;

c. ANY INFORMATION COLLECTED AND/OR OTHERWISE OBTAINED BY RSA AND SUBSEQUENTLY DELIVERED TO CUSTOMER PURSUANT TO THE FAS IS PROVIDED "AS IS" AND RSA MAKES NO WARRANTIES OR REPRESENTATIONS AS TO THE ACCURACY OR VERACITY OF THE INFORMATION.

d. RSA DOES NOT WARRANT THAT INFORMATION COLLECTED PURSUANT TO THE FAS WILL MEET ANY SPECIFIC CRITERIA, INCLUDING BUT NOT LIMITED TO COMPLIANCE WITH ANY "CHAIN OF CUSTODY AND/OR CHAIN OF EVIDENCE" PROTOCOLS, WHICH MAY BE REQUIRED FOR THE INFORMATION TO BE ADMITTED AS EVIDENCE IN ANY CRIMINAL OR CIVIL PROCEEDING BEFORE ANY JURISDICTION.

e. Disclaimer and Exclusions. Except as expressly stated in Section 6(A) above, RSA (including its suppliers, subcontractors, employees and agents) provides Services "AS IS" and makes no other express or implied warranties, written or oral, and ALL OTHER WARRANTIES ARE SPECIFICALLY EXCLUDED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ANY WARRANTY ARISING BY STATUTE, OPERATION OF LAW, COURSE OF DEALING OR PERFORMANCE, OR USAGE OF TRADE. NOTHING HEREIN IS INTENDED TO CONSTITUTE OR CREATE ANY REPRESENTATION OR WARRANTY BY RSA TO ANY THIRD PARTY, (INCLUDING END USERS), DIRECTLY OR AS A THIRD PARTY BENEFICIARY, WITH RESPECT TO ANY OF THE SERVICES PROVIDED HEREUNDER.

8. LIMITATION OF LIABILITY.

a. RSA'S TOTAL LIABILITY (INCLUDING THE LIABILITY OF ANY SUPPLIER, SUBCONTRACTOR, EMPLOYEE OR AGENT OF RSA), AND CUSTOMER'S SOLE AND EXCLUSIVE REMEDY FOR ANY CLAIM OF ANY TYPE WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH ANY SERVICES PROVIDED HEREUNDER, SHALL BE LIMITED TO PROVEN DIRECT DAMAGES CAUSED BY RSA'S SOLE NEGLIGENCE IN AN AMOUNT NOT TO EXCEED (i) US$1,000,000, FOR DAMAGE TO REAL OR TANGIBLE PERSONAL PROPERTY; AND (ii) THE PRICE PAID BY CUSTOMER TO RSA FOR THE SPECIFIC SERVICE FROM WHICH SUCH CLAIM ARISES IN THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO A CLAIM HEREUNDER, FOR DAMAGE OF ANY TYPE NOT IDENTIFIED IN (i) ABOVE BUT NOT OTHERWISE EXCLUDED HEREUNDER.

b. EXCEPT WITH RESPECT TO CLAIMS REGARDING VIOLATION OF RSA PROPRIETARY RIGHTS (INCLUDING ANY LICENSE GRANTED THEREUNDER), NEITHER CUSTOMER NOR RSA (INCLUDING RSA'S SUPPLIERS, SUBCONTRACTORS, EMPLOYEES AND AGENTS) SHALL (i) HAVE LIABILITY TO THE OTHER FOR ANY SPECIAL, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, OR INDIRECT DAMAGES (INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS, REVENUES, DATA AND/OR USE), EVEN IF ADVISED OF THE POSSIBILITY THEREOF; AND (ii) BRING ANY CLAIM BASED ON ANY SERVICE PROVIDED HEREUNDER MORE THAN EIGHTEEN (18) MONTHS AFTER THE CAUSE OF ACTION ACCRUES.

9. GOVERNMENT REGULATIONS. The Services and any technology delivered in connection therewith pursuant to this Agreement may be subject to governmental restrictions on (i) exports from the U.S.; (ii) exports from other countries in which such Services and technology may be provided or located; (iii) disclosures of technology to foreign persons; (iv) exports from abroad of derivative products thereof; and (v) the importation and/or use of such technology included therein outside of the United States (collectively, "**Export Laws**"). Diversion contrary to U.S. law is expressly prohibited. Customer shall, at its sole expense, comply with all Export Laws and RSA export policies made available to Customer by RSA. Customer represents that it is not a Restricted Person, which shall be deemed to include any person or entity: (1) located in or a national of Cuba, Iran, Libya, North Korea, Sudan, Syria, or any other countries that may, from time to time, become subject to U.S. export controls for anti-terrorism reasons or with which U.S. persons are generally prohibited from engaging in financial transactions; or (2) on any restricted person or entity list maintained by any U.S. governmental agency. Certain information, Services or technology may be subject to the International Traffic in Arms Regulations. This information, Services or technology shall only be exported, transferred or released to foreign nationals inside or outside the United States in compliance with such regulations. Certain

information, products or technology may be subject to the International Traffic in Arms Regulations ("ITAR"). This information, products or technology shall only be exported, transferred or released to foreign nationals inside or outside the United States in compliance with ITAR.

10. NOTICES. Any notices permitted or required under this Agreement shall be in writing, and shall be deemed given when delivered (i) in person; (ii) by overnight courier, upon written confirmation of receipt; (iii) by certified or registered mail, with proof of delivery; (iv) by facsimile transmission with confirmation of receipt; or (v) by email, with confirmation of receipt. Notices shall be sent to the address, facsimile number or email address set forth above, or at such other address, facsimile number or email address as provided to the other party in writing.

11. INDEPENDENT CONTRACTORS. The parties shall act as independent contractors for all purposes under this Agreement. Nothing contained herein shall be deemed to constitute either party as an agent or representative of the other party, or both parties as joint venturers or partners for any purpose. Neither party shall be responsible for the acts or omissions of the other party, and neither party will have authority to speak for, represent or obligate the other party in any way without the prior written approval of the other party.

12. MISCELLANEOUS. This Agreement (i) shall constitute the complete statement of the agreement of the parties with regard to the subject matter hereof and (ii) may be modified only by a writing signed by authorized representatives of both parties. Except for the payment of fees, neither party shall be liable under this Agreement because of a failure or delay in performing its obligations hereunder on account of any force majeure event, such as strikes, riots, insurrection, terrorism, fires, natural disasters, acts of God, war, governmental action, or any other cause which is beyond the reasonable control of such party. RSA shall not be liable under this Agreement because of failure or delay in performing its obligations hereunder on account of Customer's failure to provide timely access to facilities, space, power, documentation, networks, files, software, and Customer personnel that are reasonably necessary for RSA to perform its obligations. Neither party may assign this Agreement to a separate legal entity, without the other party's written consent. Neither party shall unreasonably withhold or delay such consent; provided, however, that such written consent shall not be required if (i) either party assigns this Agreement to a separate entity in connection with a merger, acquisition, or sale to such other separate entity, unless the surviving entity of the merger, acquisition, or sale of assets is a direct competitor of the other party. Nothing herein shall limit RSA's right to assign its right to receive and collect payments hereunder. This Agreement is governed by the laws of the Commonwealth of Massachusetts, excluding its conflict of laws rules. The Parties hereby: (1) irrevocably commit to the exclusive jurisdiction of the federal and state courts located in the Commonwealth of Massachusetts for the purpose of any suit, action or proceeding arising out of this Agreement, the subject matter hereof or any of the transaction contemplated hereby brought by either Party or its successors or assigns; (2) waives, and agrees not to assert, by way of motion, as a defense or otherwise, in such suit, action or proceeding, to the fullest extent permitted by applicable law, that the suit, action or proceeding is brought in an inconvenient forum, that the venue or the suit, action or proceeding is improper, that that this Agreement, or the subject matter hereof or any of the transactions contemplated hereby may not be enforced in or by such courts; (3) waives the right to trial by jury of any suit, action or proceeding; and (4) waives any right, claim, or entitlement to any punitive or exemplary damages whatsoever, except as otherwise provided in this Agreement. All terms of any purchase order or similar document provided by Customer, including but not limited to any pre-printed terms thereon and any terms that are inconsistent, add to, or conflict with this Agreement, shall be null and void and of no legal force or effect. No waiver shall be deemed a waiver of any prior or subsequent default hereunder. If any part of this Agreement is held unenforceable, the validity of the remaining provisions shall not be affected. In case of any conflict between an Exhibit and this Agreement, the Exhibit shall control. Each Party will comply with all applicable laws and will obtain, and will maintain in full force and effect, all licenses, permits, approvals, and other authorizations that are necessary or required to perform its obligations under this Agreement. The titles and headings of the Sections and other subdivisions of this Agreement are for convenience of reference only and shall not modify, define or limit any of the terms or provisions of this Agreement. This Agreement has been drawn up in and shall be construed in accordance with the English language.

EXHIBIT – A

FRAUD ACTION SERVICE DESCRIPTION

This Exhibit A specifies the components which form part of the FAS.

From the FAS Activation Date, each selected component of the FAS shall be provided with respect to the Customer Domains and the Territory specified in the applicable Section of this Exhibit A.

A Customer Domain shall be extended by reference to include any services provided by the Customer under a domain name that includes the exact words of the Customer Domain(s) provided always that (1) the RSA project team shall be required to work with not more than one Customer project team; and (2) that the bank or other financial accounts which form the target group of fraud campaigns directed at each variation of the Customer Domain are also based in the Territory.

A. General Fraud Action Service features

1. Hosting, Hardware and Software
RSA will provide all hardware, software, database and communications equipment necessary to support the FAS as described in this Exhibit A.

2. The RSA eFraudNetwork database
Customers who subscribe the Anti-Phishing Service component shall benefit from RSA's use of eFraudNetwork data, for the purpose of early detection of phishing attacks as well as for the purpose of taking certain action against such phishing and/or pharming attacks.

3. Documentation
RSA will deliver all necessary documentation required to properly benefit from the FAS.

4. 24x7 Availability
The FAS is operational 24 hours per day seven days per week. The fraud specialists at the AFCC will provide support prior to an attack, during an attack and after the attack as well.

5. Reporting - Dashboard/Portal
In addition to Incident specific reporting, RSA will provide and maintain access to a secure web based dashboard or portal (herein the "Dashboard") that will report all known attacks and provide information about these together with any additional information relating to the Anti-Pharming, Anti-Trojan and Anti-Phishing Services.

B. Fraud Action Service Specific Components

I. Anti-Phishing Service

From the FAS Activation Date, the Anti-Phishing Service shall be provided with respect to the following Customer Domains:

- *INSERT CUSTOMER DOMAIN NAMES as set forth in the applicable Service Setup Form*; and in the following Territory:

- *TERRITORY as set forth in the applicable Quotation*

1. APS Incident Alerts for Customer Domain(s)

1.1 Customer will receive alerts via RSA's 24X7 Anti-Fraud Command Center.

1.2 RSA's detection is based on, spam and abuse reports, email decoys and email scanning of tens of millions of emails originating from enterprise email gateways, desktop users and selected large ISPs every day.

1.3 Alerts are provided via email based on pre-determined Customer specific escalation procedures as notified to RSA in the course of the FAS setup.

1.4 The Dashboard will provide summary information including: number of phishing attacks to date; number of closed APS Incidents since the launch of the Anti-Phishing Service; Number of live (active) APS Incidents since the launch of the Anti-Phishing Service; number of APS Incidents open/closed in the last 24 hours.

2. "Taking Action" – APS Incident Shut down; Forensic Work; and Counter Measures (with respect to a domain or website which is hosting a phishing attack or potential Customer Domain abuse)

2.1 "Taking Action" – APS Incident Shut down

(a) RSA will analyze each phishing attack and identify the spoofed websites hosting the phishing attack and their respective Internet Service Providers ("ISP(s)").

(b) RSA will make best efforts to contact the ISPs, and/or the entity responsible for the spoofed website, on Customer's behalf and alert them of the spoofed website and request that this be shut down. If the spoofed website has been incorporated within a legitimate website, RSA will also make commercially reasonable efforts to notify the owner of the legitimate website of the existence of the spoofed pages within such website as well as of the fact that the hosting ISP has been requested to shutdown the website (it should be noted that whenever a phishing attack originates from a compromised personal computer it is highly unlikely that RSA would be able to directly contact the owner of such computer).

(c) RSA may attempt to approach each ISP and send it a cease and desist. Customer may require that RSA obtain its prior consent before sending any cease and desist notices.

2.2 "Taking Action" – APS Incident related Forensic Work

(a) Wherever reasonably possible RSA will attempt to extract valuable information from the spoofed website server hosting a phishing attack. While this cannot be guaranteed, in the past RSA has extracted data, including counters of the number of users that submitted information to the fraudulent site, and in several cases the actual full list of stolen data collected by the fraudster was obtained by RSA (containing the user names, passwords, PINs etc. of all the phishing victims).

(b) RSA's forensic work is performed using knowledge RSA has gathered through its alerts infrastructure and network of customers, allowing it to implement lessons learned from one phishing attack to the next. This provides RSA with an early insight of the technology used in phishing attacks, especially when a fraudster is still in "QA" mode, i.e. testing a fraudulent website prior to launching a web campaign in order to attract unsuspecting end users to the spoofed website.

2.3 "Taking Action" – APS Incident Counter Measures

(a) "Baits" counter-measures utilize RSA's Randomized Credentials Technology ("RCT"), using randomized generated accounts.

(b) RSA will where reasonably practicable activate its baits counter measures in coordination with Customer. The exact RCT behavior will be determined based upon the template set of end user credential parameters and configuration information mutually agreed by the Customer and RSA during the kick off meeting. Customer will have approved the rate and velocity of use of the RCT.

(c) RSA will provide the Customer with the details of the bait records that were submitted to the fraudulent website. These reports will be added to the phishing attack assessment reports as provided pursuant to Section A(5) of this Exhibit A.

(d) If Customer elects to use baits, Customer and RSA will work in advance and adjust Customer's own fraud detection system to monitor the baits data that is fed by RSA to the fraudulent website.

(e) for the purpose of the counter-measures described above, the Customer will provide RSA with not more than one template set of end user credentials for the purpose of creating the counter measures data files.

3. Blocking of phishing URLs by RSA's ISP Network

Customer hereby acknowledges and agrees that RSA may at its discretion forward all confirmed phishing attack URLs to its network of ISP partners (which includes but is not limited to Microsoft and AOL and other ISPs who join the network), for the purpose of blocking access to such fraudulent URLs.
Furthermore, Customer hereby authorizes RSA to forward a list of Customer's legitimate URLs to its blocking Network partners (herein "Blocking Partners").

II. Anti-Pharming Detection and take down

Pharming (also referred to as DNS Poisoning or DNS Spoofing) is a method of conducting financial fraud. A Pharming attack redirects web-surfers that try to reach a known Customer website to a spoofed web site instead. Users are redirected to an exact replica of the legitimate Customer website and the fraudsters then 'harvest' legitimate end user credentials in mass numbers. The Anti-Pharming Service identifies DNS Poisoning or Spoofing Attacks by using dedicated servers that monitor the internet in search for poisoned DNS servers. RSA's Anti-Pharming Service is geared toward three of the possible four locations where DNS routing can be altered by fraudsters: ISP DNS servers, DNS Root servers, and authoritative name server locations where the large scale attacks are typically targeted.

As part of the Anti-Pharming Service setup, Customer will provide RSA with a list of up to twenty (20) legitimate domains and their resolving IP addresses (the RSA project team shall not be required to work with more than one Customer project team).

The Anti-Pharming Service then constantly queries the root DNS servers; the authoritative DNS servers; and several large ISP DNS servers to check for valid name server and IP responses that correctly match with the Customer's legitimate domains as notified to RSA by the Customer.

The Anti-Pharming Service alerts RSA's 24x7 Anti-Fraud Command Center ("AFCC") if a suspicious match, that is not included in the legitimate list, is found.

The Service also scans several large ISP DNS servers to verify that their cached data is not poisoned. If a Pharming Attack is detected and confirmed by RSA, Customer will be alerted by RSA.

III Anti-Trojan Service

From the FAS Activation Date, the Anti-Trojan Service shall be provided with respect to the following Customer Domains:

- *INSERT CUSTOMER DOMAIN NAMES as set forth in the applicable Quotation*; and in the following Territory:

- *TERRITORY as set forth in the applicable Quotation*

The Anti-Trojan Service described herein is a service, in general, under which RSA provides or facilitates the identification and analysis of Crimeware targeting customers of the Anti-Trojan Service, and if possible as a result of such analysis, takes steps to limit the effectiveness of such Crimeware. Such steps may include blocking infection points and/or shutting down key infection and drop sites.

The Anti-Trojan Services include the following features:

1. Identification of Crimeware

- RSA will use reasonable commercial efforts to provide Customer with near-real-time Crimeware identification based upon information received from RSA's Anti-Virus technology company partner network ("AV Partners") and RSA's proprietary internal Crimeware detection technologies.
- RSA, together with its AV Partners, will use reasonable commercial efforts to identify different variants of Crimeware.

2. Analysis of Crimeware

When specific Crimeware is identified by, or made known to, RSA, a detailed analysis of the Crimeware will be made available by RSA to Customer. Such analysis will be in a format generally provided by RSA to its customers and may include one or more of the following: the Crimeware method of infection and propagation; what user information is gathered and/or transmitted by the Crimeware; which processes within an infected system are compromised by the Crimeware, how the Crimeware command-and-control operates, and the destination drop sites to which stolen credentials are sent. In addition, when specific Crimeware is identified by, or made known to, RSA:

- RSA will analyze fraudster modes of operation including but not limited to: Key-loggers, screen-scrapers, session hijackers, local pharming
- RSA will seek to identify the communication methods employed by the operator(s) or handler(s) of deployed trojans (or other similar types of Crimeware)

3. Blocking of Infection Points

RSA will use reasonable commercial efforts to liaise with its network of "Blocking Partners" (which consists of a network of Internet Service Providers and other entities) in order to provide information which will enable these partners to limit or block access to websites which are confirmed Crimeware infection points.

Customer hereby acknowledges and agrees that RSA may at its discretion forward all confirmed infection website information (including but not limited to the relevant URL) to its network of Blocking Partners for this purpose.

4. Shutdown of Infection Points, Drop Sites, or Command and Control Points

(a) RSA will analyze Infection Points, Drop Sites, Update Points, or Command and Control Points and seek to identify the operator of the hosting website and/or their respective Internet Service Providers ("ISP(s)").

(b) RSA will make commercially reasonable efforts to contact the ISPs, and/or the entity responsible for the hosting website, on Customer's behalf, and alert them of the Infection Point or Drop Site

and request that this be shut down. If the hosting website has been incorporated within a legitimate website, RSA will also make commercially reasonable efforts to notify the owner of the legitimate website of the existence of the pages hosting the Infection Point or Drop Site within such website as well as of the fact that the hosting ISP has been requested to shutdown the website (it should be noted that whenever a Trojan attack originates from a compromised personal computer it is highly unlikely that RSA would be able to directly contact the owner of such computer).

(c) RSA may attempt to approach each ISP and send it a cease and desist. Customer may require that RSA obtain its prior consent before sending any cease and desist notices (this will be specified in the FAS set-up form).

5. ATS Forensic Work

Whenever reasonably possible RSA will attempt to obtain Information from the Crimeware Drop Sites and provide this to Customer where RSA, in its sole discretion, deems this Information to be of value to the Customer. Without making any warranties or representation as to the availability of useful Information and by way of example only, this may include without limitation lists of compromised account holder credentials appropriated by the fraudsters (such as account holder usernames, passwords, etc).

6. Reporting - Dashboard

RSA will maintain and provide access to the Dashboard which will provide Customer with near real time alerts of all newly reported forms of Crimeware, together with detailed information about these and the methods of infection or known drop sites.

Upon the prior written request of Customer, RSA will be available for a weekly team meeting with dedicated project manager.