BASED ON INFORMATION PROVIDED BY MSWM BEGINNING IN 2007 AND THE CURRENT METASWARM.COM CORPORATE WEBSITE (AS OF JUNE 11, 2013).

HIGHLIGHTS

MetaSwarm ("MSWM") is a software development firm focused on being a leader in Internet personal information assurance and e-commerce anti-fraud and anti-spam. Key highlights of the company include:

1. Proprietary MetaSwarm technology that MSWM management believes is superior to any of the competing technologies used in the industry today;
2. Over 34 innovative patents pending;
3. Strong core management and technical teams comprised of talented, experienced personnel with expertise covering the gamut: gifted technologists, tested business development, and marketing veterans, and seasoned financial expertise;
4. Company with a mission to build Internet trust;

MetaSwarm is a software company focusing on specialized personal information assurance solutions, including validated messaging services, validated transaction services, anti-fraud and anti-spam products, and relationship analysis solutions for the Internet e-commerce markets. MetaSwarm's primary focus is applications and services for cell phones, and other personal wireless devices; additionally, MetaSwarm products are also available for legacy desktop systems. MetaSwarm's mission is to enable consumer trust in online communications and transactions -- a trust required for the continued growth of global e-commerce.

MetaSwarm has filed over 34 innovative Patents Pending for their proprietary technologies that make possible the company's redefinition-of-the-art *Essurance* solution -- a solution that will seek to build Internet trust. MetaSwarm's goal is to deliver peace-of-mind to Internet users -- an Internet safeguarded against fraudulent and unsolicited messages (spam), and against phishing messages and pharming websites—either in conjunction with Service Providers or directly from MetaSwarm Aggregation Centers (AggCenters).

MetaSwarm's strategy is to develop product rollout activities in select markets with its initial Essurance products. MSWM is planning to set up AggCenters in China; through these AggCenters, MetaSwarm can support users of the Essurance system globally. AggCenters will provide Internet users with access to validated messaging and validated transaction services to Government, ISPs, Enterprises, and other Organizations.

In addition, MetaSwarm is seeking partnerships with global Internet companies, including Google, Yahoo, MSN, and eBay. MetaSwarm technologies and products can solve current major problems that such global Internet companies have and can add value to their product offerings.

THE OVERALL MARKET

1. There are 2.5 billion cell phone users worldwide; with more than 41 million new users per month. The ubiquitous nature of wireless Internet devices, and the corresponding number of users, make them attractive targets for phishers, pharmers, and spammers.
2. The Internet provides a cheap and efficient medium for phishing messages and pharming websites that lead to identity theft as well as to outright fraud.

3. There have been no effective methods for controlling Internet fraud, phishing, pharming, pornography, or the voluminous commercial messages.
4. Phishers and pharmers are technically sophisticated and are able to automate the processes that make the Internet a cheap advertising medium, and are able to overcome the few attempts made to control them.
5. The inherent attributes of cell phone based messaging and Internet access in conjunction with validated messages make it possible for MetaSwarm products to deliver a safe online experience.

TARGET MARKET AND CUSTOMERS

The target markets of validated messaging, validated transaction services, anti-fraud, reputation management, and monitoring, filtering, and control comprise customers of different levels based on their particular needs. MetaSwarm recognizes the following customer groups:

- Individuals – wireless Internet users, primarily cellphone based, who need certain and immediate validation of messages, financial transactions, and websites.
- Corporations/Enterprises – who need certain and immediate validation of messages, financial transaction services, and websites; and who need to maintain the integrity of their corporate identities.
- ISPs/IDCs – who need certain and immediate validation of messages and websites, who need to maintain the integrity of their corporate identities, and who need to protect individual and corporate customers from fraud and identity theft.
- Authority – who need certain and immediate validation of messages and websites, who need to maintain the integrity of their organizational identities, who need to protect individual and corporate customers from fraud and identity theft, and who need to send official messages without the fear of fake or unauthorized "official" messages reaching recipients.
- All groups need certainty that messages and websites that they access are what they purport to be. They need confidence in the information they obtain about originators of messages and websites, so that they can make informed decisions.

MARKET SEGMENTS, SOLUTIONS, AND COMPETITION

MetaSwarm recognizes four market segments based on the type of problem that faces Internet users today. The segments are:

- Validated Messaging
- Validated Transaction Services
- Message Management
- Monitoring, Filtering, and Control of Electronic Messaging

The MetaSwarm **Essurance** system provides solutions to these problems. Though competitive products exist for some aspects of these problems, they are ineffective and they lack a comprehensive solution for the broader arena of electronic communications on the whole.

ONLINE FRAUD

Online fraud encompasses phishing and pharming (fraudulent websites). Phishing messages attempt to fool recipients into providing private information, such as:

- Social security numbers
- Credit card numbers

- Banking information
- Account numbers, user IDs, PINs, and passwords

The phisher's intent is to collect the private information for use in fraudulent schemes. Links in phishing messages and fraudulent, or pharming, websites lead recipients to fake web pages that appear to be from valid organizations. Recipients enter private information in the fake web pages, not realizing that the information is being passed to a phisher rather than to a valid organization.

According to the Phishing Trends Report by the Anti-Phishing Work Group (APWG), the number of unique phishing attacks increased 139% from 12,845 in January 2005 to 17,877 in January 2006. During the same period, the number of pharming websites increased from 2,560 to 9,715 -- a 379% increase.

The financial services industry (including banks, brokerage houses, e-commerce companies, and insurance companies) is the most targeted sector for phishing attacks. Gartner Research estimates that phishing schemes alone have cost banks US$1.3 billion; and various industry analysts estimate that spending to thwart phishing attacks will be in excess of US$10 billion annually by 2007.

Until 2004, phishing was almost unknown outside of the US, UK, and Australia. Today it is spreading to developed countries all around the globe. Indeed, in June 2004, two major German banks, Deutsche Bank and Postbank reported the first phishing attacks targeted at their customers.

In addition, according to the APWG report, 101 brands were hijacked by phishing attacks in just the one month of January 2006. In brand hijacking, a phishing message or pharming website appears to be from a legitimate institution, either a corporation (generally, a financial institution) or now even a government agency (such as the Internal Revenue Service).

Brand hijacking can cost the target institution not only in financial terms but also in terms of its reputation. Institutions can only react to brand hijacking when it is discovered. Even though discovery can take place within days, it's long enough to make a financial and reputational impact.

To date there have been no technological constraints to keep phishing from spreading to any country, or in any language in which e-commerce is conducted.

ESSURANCE VALIDATED MESSAGING—THE METASWARM SOLUTION TO ONLINE FRAUD

With the Essurance system, clients can make validated mass mailings. Even though they are mass mailings, clients can customize them for individual users using a single validation block. The validation block is in the form of Partner Lists, which clients use to identify valid messages as well as valid websites.

Essurance is entirely deterministic, with zero chance of identifying a phishing message as being a valid communication from a client. Using the MetaSwarm validation technologies provides a lightweight, easily implemented, and elegant solution against the modern plague of phishing:

- Partner List: MetaSwarm uses the Partner List to specify valid addresses and other validation properties of its outgoing messages, as well as to identify valid websites. Each MetaSwarm client, such as a bank, uses the Partner List as a repository for its valid information—its valid URLs, valid partner URLs, profiles of its websites, profiles of e-mailings, and Partner List activation dates and times. The Partner List contains information relating to the corporate or government client in general, but may also have information on a per-mailing or mass-mailing basis.
- notPhish tags: These tags are inserted into client messages and websites, and specify the applicable Partner List to be used to verify their integrity. The tags allow mass customization of messages, while allowing validation of the entire mass mailing with one validation block.

- notPhish plug-in: The notPhish plug-in, distributed by a client to its customers, adds a notPhish icon onto the customer's cell phone or computer browser and email application window. The plug-in validates messages and websites against the Partner List at the customer's computer and uses the icon to indicate a message's or website's validity to the customer. Only an exact match to the Partner List is valid.

Essurance uses proprietary software to verify that authorized bulk mailings from valid organizations are unmodified in any way. This capability protects a valid client's mailings not only from phishing and spamming but also from malicious modifications, such as the addition of objectionable textual or graphical content.

With Essurance, clients can use Partner Lists to target automated discovery of phishing and pharming websites. Clients can use automated discovery to ensure the integrity of their reputation by protecting against brand hijacking. Clients can use their trademarks and other corporate identification keywords to perform highly targeted and automated searches for messages and websites that use them and to determine whether such use is authorized or not.

In a similar manner, clients can use Essurance to determine relationships between their organization and external organizations. For example, a client could learn that the host of its web services is also host to organizations of questionable integrity. Such a relationship, though indirect, could be benign or it could undermine the client's reputation. However, given the information, the client can act as it deems appropriate.

Further, Essurance can do reputational analysis of organizations based on HyperSwarm relationship models, and it can provide links to organizations such as Dun & Bradstreet, Barron's, and Rutgers. Users with the notPhish plug-in would click on the validation icon to obtain an organization's reputational analysis and to obtain information about that organization. Such information would enable users to determine whether or not to pursue interactions with a particular organization.

MARKET OPPORTUNITY: CREDIT CARD AND BANKING FRAUD

Credit card and banking fraud encompass identify theft instances in which a perpetrator uses stolen private information to perform financial transactions. The private information may have been stolen through online phishing or pharming scams, or through man-in-the-middle attacks—whether online or physically (as in observing a user enter a PIN at an ATM and then stealing the ATM card).

Multiple mechanisms exist for authenticating a user, such as using passwords, software tokens, biometrics, SmartCards, certificates, and two-factor (in which more than one thing is required to authenticate a user). Mechanisms such as passwords and software tokens are subject to theft and are therefore not entirely secure. The other mechanisms are costly (biometrics, SmartCards, two-factor) or unwieldy (certificates) for large-scale implementation.

With the rise of online sales and online banking, preventing credit card and banking fraud is of paramount concern to users and financial institutions, with the financial institutions carrying the burden for implementing expensive authentication mechanisms for lack of a true solution.
Essurance Validated Transaction Services—the MetaSwarm solution to credit card and baking fraud

With the Essurance system, clients can leverage the increasing use of cell phones to provide Validated Transaction Services. The same validation mechanism that the Essurance system uses to provide Validated Messaging serves as the basis for Validated Transaction Services.
The Validated Transaction Service is a two-factor system in which the cell phone replaces the key fob used by two-factor authentication systems, such as RSA.

A bank or credit card customer registers with the bank or credit card company to use the Validated Transaction Service. When the customer initiates a transaction, at an ATM for example, after entering the PIN, the bank sends a validated text message to the customer's cell phone with a passcode. The customer

then has a limited time (typically 30 to 60 seconds) to enter the passcode at the ATM to complete the authentication.

The Essurance Validated Transaction Service is a simple solution. The key is the validated message from the bank or credit card company. Because the message is validated, the customer knows with certainty that the message with the passcode really is from the specific bank or credit card company. Also, the bank and credit card company can be relatively certain that the person who entered the PIN and holds the cell phone that receives the validated message is the same.
In addition, the validation can take place for each transaction that the customer performs. This capability totally removes man-in-the-middle attacks in which authenticating information is intercepted between multiple transactions during the same session.

CREDIT CARD AND BANKING FRAUD COMPETITION

In the two-factor authentication arena, financial institutions, such as banks, distribute key fobs to customers who request them. The fobs and the synchronization servers are expensive for the bank. Their use is limited to customers who request the additional security or for customers using certain banking services, such as online wire transfers. Because of its limited use, the security that two-factor authentication provides the institution is also limited.

For the customer, carrying a key fob may be an inconvenience. The customer may also have the inconvenience of carrying multiple key fobs, one for each pertinent account in multiple financial institutions. With the Essurance Validated Transaction Service, the customer can register with any number of financial institutions and have them send validated messages to the same cell phone.

MARKET OPPORTUNITY: MESSAGE OVERLOAD

Spam is the Internet's version of annoying junk mail, telemarketing calls during dinner, crank phone calls, and leaflets pasted around town, all rolled up into a single annoying electronic bundle.

According to IDC estimates, the number of spam messages sent on an average day worldwide jumped from 4 billion in 2001 to 17 billion in 2004 to 33 billion in 2006. Today, approximately 40% of all email on the Internet is spam—and spam volume continues to grow.

Productivity loss due to spam has become an issue for organizations where, on average, each email user spends 10 minutes a day dealing with spam, and IT staffs spend 43 minutes a day dealing with it. A study by leading communications research firm Ferris Research indicates that corporate organizations incur costs for spam totaling between $9 and $10 per user per month. According to Ferris Research estimates, spam cost about $50 billion globally in 2005, $17 billion of which was the cost to US businesses.

Even in spite of the new laws and the current anti-spam technology, the spam volume is increasing. In fact, unsolicited commercial email (spam) is increasing at such an alarming rate that it is threatening to render email useless as a form of communications. Already there is an increase in instant messaging (IM) as a way to bypass email use. However, IM use will also increase corporate costs as corporations move to satisfy requirements for IM tracking and archiving. In addition, IM is subject to spam; as IM use increases so will IM spam as spammers seek new targets.

Mobile short message service (SMS) is also subject to spam, as is evident in Asia and Europe where SMS is used more than in the US.

Although the market for email anti-spam products is saturated, end users see the existing products as being basically ineffective. Corporations and consumers are still spending $1B US annually in hopes that these products will somehow help alleviate their problem and thus reduce their operational costs. Various industry analysts estimate that spending will be in excess of $10B US annually by 2007.

Most anti-spam products focus on email spam. IMlogic, recently acquired by Symantec, is MSWM's closest competitor for IM. However, the product is also based on the same techniques as for email spam and is equally ineffective. In the SMS arena, there exists the Bayesian approach, which is similar to that used for email spam, and there is the "postage paid" approach. Besides the unpopularity of the postage paid approach, the technique is not effective because it either stifles advertising or makes it available only to groups that can pay a lot of money (the big players).

Message management, however, is more than identifying and blocking spam. It encompasses managing messages overall, including sorting and classifying messages and providing enough information for users to set filters adequate for their needs. Essurance is about comprehensive message management.

ESSURANCE – THE METASWARM SOLUTION TO MESSAGE OVERLOAD

With the Essurance system, clients can determine whether email, SMS, and IM/IRC messages are bulk or non-bulk (or unique). If messages are bulk, Essurance further enables clients to determine whether the messages are conforming bulk (such as newsletters) or non-conforming (such as spam and phishing messages).

Using Bulk Message Envelope (BME) technology (see Section A.5), Essurance reduces a message to an invariant form and then creates hashes from it. The hashed result is the essence of the message, stripped of all elements that spammers or phishers may include in the message. This greatly minimizes the effort required to keep up to date with spammers and phishers.

Algorithmic technologies preclude human interaction in the processing of messages. This removes the subjective aspect of classifying messages as spam and preserves privacy.
Reducing messages to their hashed form is fast. Subsequent BME analysis takes place on the hashed results of messages, which are reduced in size by 83% and thereby minimizing the computational resources required to analyze large numbers of messages.

There is no risk of rejecting good messages. BME technology clearly recognizes unique messages. Also, the user interface allows individuals and system administrators to easily classify bulk messages that are acceptable to one or more individuals or organizations.

BME technology is completely language-independent. It can process messages written in any language, separately or together.

Essurance message management becomes more efficient with increasing message volume. BMEs make possible easy and efficient management of any number of messages, from 1 to 1 billion. As BME analysis of incoming messages takes place, Essurance can block unacceptable or undesirable messages from being delivered.

In addition, cluster analysis enables Essurance to continually generate blacklists that reflect the actual and current real-time state of spam on the Internet. It can generate blacklists—in minutes—consisting of thousands and tens of thousands of spammer domains. These blacklists may be made available, separately or in aggregated form, to individuals or organizations too small to generate blacklists large enough to be useful.

MESSAGE MANAGEMENT COMPETITION

The competition is only about anti-spam—not about message management.

There are quite a number of anti-spam products currently deployed in the market, the major competitors being Symantec, Sybari, and Barracuda. However, we believe that Essurance delivers superior capabilities

and performance; especially when compared to competitors in the marketplace today. Generally, the competition focuses on:

- Bad words
- Bad styles
- Existing links to a website in a blacklist, where the blacklists are generated in large part by manually-identified spam messages—which is highly inefficient and demonstrated ineffective.
- In the following paragraphs, we summarize MSWM's competitor's technologies for anti-spam, and describe their limitations and disadvantages as compared to the Essurance anti-spam functions.

COMPETITOR SOLUTIONS

Today, MSWM's competitor's anti-spam solutions may ease the problem, but only temporarily; and generally at the price of false positive identifications. These anti-spam solutions are essentially filters that target specific aspects of spam email. Competing anti-spam solutions usually use one or more methods, including:

- Bayesian filters
- Textual analysis, including keyword scanning
- Heuristic (style) analysis
- Semantic/Intent analysis
- White lists
- Black lists
- Challenge response
- Network verification
- Disadvantages and Limitations

The methods used by competitive anti-spam solutions have disadvantages that restrict their usefulness in any of various ways, including:

- The amount of effort to keep up to date with spammers that continually evolve their techniques in response to anti-spam solutions.
- The human interaction required to define spam and non-spam, which is not only subjective (spam to one person is not spam to another) but it intrudes on the privacy of the messages.
- The intensive computational resources required to analyze a given method's rule set.
- The higher risk of inadvertently rejecting good email.
- Language-dependence, which is a major restriction in a space that is truly global.
- The lack of a comprehensive or broader view of spam interconnections.
- Based on Symantec's corporate history, market coverage, and customer impact, we believe Symantec's Brightmail System to be MSWM's major competitor in the marketplace. We have written a head-to-head comparison between Essurance and Symantec's Brightmail to highlight MSWM's advanced technology, superior effectiveness, and efficiency as an anti spam solution.

MARKET OPPORTUNITY: MONITORING, FILTERING, AND CONTROL

The Internet is the new frontier for interpersonal relations. Children are logging on to the Internet more than ever before, searching for interesting information, playing games, chatting with friends, and getting help with schoolwork. The Internet has opened up a whole new world for them.

The online world, like the real world, is made up of a wide array of people. Most are decent and respectful, but some may be rude, obnoxious, insulting, or even mean and exploitative. Areas full of sex, violence, drugs, and other adult themes are another possible danger for children. The fact that crimes can be committed online, however, is not a reason to stop children from using Internet services. Children need parental supervision and common sense advice on how to make their experiences with the Internet happy, healthy, and productive.

In the wake of increasing concern by parents of net-savvy children about objectionable content, limiting access to objectionable information has a growing demand.

In the corporate world, corporations have similar problems with employee access to inappropriate messaging and websites. In addition, corporations may want to restrict access to particular protocols. Corporations and government agencies also want to be able to discover brand hijackers as soon as possible.

Today, due to the limited availability of efficient technology, most authorities rely on simple computer search tools and large amounts of manpower to compete with and fight against legions of hackers and online criminals. Because of the complexity and constantly evolving nature of Internet technologies, the effectiveness and efficiency of the current generation of tools is not meeting the needs of authorities to suppress fraudulent use.

There is a huge demand among Government Authorities around the world for efficient computing tools that help fight Internet fraud. Especially in countries that tightly regulate Internet usage and undesirable content, and that strictly prohibit fraudulent messages.

ESSURANCE – THE METASWARM SOLUTION TO MONITORING, FILTERING, AND CONTROL

With the Essurance system, clients have available to them sets of properties for messages and websites. For messages, properties include:

- Transmission properties, including:
- Sender names
- Recipient names
- Domains
- Number of relays used
- Timestamps
- IP addresses
- Routing information
- Hosts
- Construction properties (also referred to as heuristics or styles), such as use of:
- Invisible text
- Scripts (such as JavaScript)
- HTML tags

- Content-based properties, such as:
- Content classification (non-bulk, conforming bulk, non-conforming bulk)
- Content categorization (religious, political, pharmaceutical, pornographic, financial, other user-defined categories)
- Content sub-categorization (user-defined tokens of interest)
- Relational properties that indicate how a message relates to other messages or to websites with respect to any property
- For websites, properties include:
- Hosting properties, including:
- Protocol use
- Port use
- IP address(es)
- Owner or third-party host
- IP address(es) for third-party host
- Network service provider (NSP)
- Internet service provider (ISP)
- Hosting service provider
- Routing information
- Content-based properties, such as:
- Multiplicities (identical or substantially similar to other websites)
- Content categorization (religious, political, pharmaceutical, pornographic, financial, other user-defined categories)
- Content sub-categorization (user-defined tokens of interest)
- Relational properties that indicate how a website relates to other websites or to messages with respect to any property

With Essurance, clients can monitor, filter, and control access to websites and manage messages based on any one property or any combination of properties.

MONITORING, FILTERING, AND CONTROL COMPETITION

At the Corporate/Enterprise level, firewalls represent the solutions for monitoring and controlling corporate access to websites and messages. MicroTrend, Symantec, and Trustix are three of the major players in this arena. With respect to messaging, the firewalls rely entirely on keyword analysis, and/or on blacklists. For websites, they rely almost exclusively on blacklists without any idea of the content or reputation of the websites in the blacklist. Firewalls rely on the blacklist providers, who build the blacklists manually, thereby presenting the problem relating to the currency and validity of the blacklist entries. Manually built blacklists are never up-to-date and are never complete because of the sheer volume of websites, and the human attention and language required to do it.

Essurance is automated and the website and message classification can be fine grained. That means that corporate users can know what to block and what not to block. Essurance can automatically manage it. The key element is determining what a mass mailing is and what is not. Essurance makes such determinations deterministically.

At the Home level, parental control is the primary issue. A large number of parental control products exist, including:

- NetNanny
- McAfee Parental Controls
- Norton Parental Controls
- Cyber Patrol
- Child Safe

The methods used by competitors have disadvantages that restrict their usefulness in several ways, including:

- The human interaction required to populate their blacklists, which are inherently subjective. In some cases, parents have to submit blacklist candidates to the product vendor for analysis and subsequent listing in the blacklist.
- Long update cycles, leaving time slots for access to unacceptable websites.
- The lack of control over messaging.
- The lack of simple user interfaces.
- As the effective answer to parental control, Essurance excels where other methods are limited:
- Behavioral Envelope (BE) technology (see Section A.5) reduces a message or a website to an invariant form and then creates hashes from it. The hashed result is the essence of the message or web site, stripped of all non-communication elements. The hashed messages and websites enable comparisons and the categorization by BE.
- Algorithmic technologies preclude human interaction in the processing of messages and websites. This removes the subjective aspect of classifying messages and websites.
- Clustering mechanisms through BE analysis enables the fast generation of large annotated blacklists—blacklists containing thousands and tens of thousands of entries. The annotations identify the content type for each entry in the blacklist.
- A simple user interface enables parents to select the content types to be blocked—whether the content type is being accessed via website or message.
- Block or notify of websites and messages based on interest profile targets, such as "like match.com".

The Essurance blacklists are continually updated real time at AggCenters. All updates are available to parents at any frequency: weekly, daily, hourly, etc.

FUTURE PRODUCTS AND SERVICES

MetaSwarm believes that the growth of Internet e-commerce is non-stop. Internet trust will be a challenge to the industry. Hackers, Internet thieves, and any other attackers will never cease their exploitation on the Internet.

Essurance will play a very important role in the Internet world as a gatekeeper, preventing phishers from spoofing message communications and websites of MSWM's corporate customers. In time, Essurance will become a necessary security measurement for all major Financial Institutions, Government, and large

Corporations. We believe that online validation of any e-commerce, e-trading, and even serious business will become part of standard operating procedures.

MetaSwarm will extend its technology-proven and market-proven anti-fraud, anti-spam, and relational analysis solutions to all these demands and, further, explore more business opportunities, such as:

- Validation services for local businesses (second tier validation)
- Anti-click fraud tools
- Trusted search capabilities
- Reputation management platform for business entities' information and credibility providers
- Blog and RSS entry validation tools
- Other validation opportunities

MARKETING STRATEGY

We believe that the Essurance platform's capability in enabling users to make informed decisions regarding validity of online transactions, messages, and websites will allow us to compete effectively in the marketplace.

In the end, what is missing from the market is certainty. Essurance is about delivering certainty. We understand that to ensure the acceptance of MetaSwarm in the marketplace, we have to build the market's confidence and trust in MSWM's technology, products, and services.
MetaSwarm will offer the Essurance services via cell based SMS/MMS and legacy desktop platforms.

Also, MetaSwarm will invest in and construct Essurance Aggregation Centers to perform:

- Partner List management services
- Online instant validation of SMS/MMS, email, website, transaction services, and other electronic message types for program participants by synchronizing the Partner List and notPhish information.
- Free notPhish plug-in software download and support for legacy desktop support
- Validated online advertisement for cell, wireless, and desktop users
- The Specialist Contractor will be responsible for:
- Promotion of the system in the Government market
- Providing pre- and post-sales support, customer requirement analysis, and customization of special system requirements
- Providing system support and maintenance services
- MetaSwarm will provide professional technical and business training to MSWM's partners and provide constant updates of the technologies and products.

SALES PLAN

The primary goal of sales for MetaSwarm is to quickly penetrate the online information assurance/ Internet security marketplace and build a sizable customer base within a relatively short period. To achieve this goal, the company will provide a flexible sales policy, including:

- OEM arrangement for specific ISPs, aggressive pricing strategy, and attractive rewards and other incentive programs.
- MetaSwarm will prioritize its market entry plans based on the level of market impact and value to the Company. We will stage the rollout efforts of MSWM's Essurance system, over the next 12-month period, in the following sequence:
- Cell phone messaging, advertising, and web access market
- Authority target market
- Corporate/Enterprise target market
- Multinational Financial Institutes, e.g. banks, credit card operators, and online payment services
- Multinational Online marketers, retailers, and shoppers
- International Fortune 10,000 corporations
- Corporate IT system contractors
- MetaSwarm's plan is to set up Essurance AggCenters in the US, Asia, and Europe, either independently or in cooperation with corporate or governmental partners.
- Partnerships
- Distributors / Partnerships
- In those countries or regions where we may encounter operational constraints due to political, religious, economical, or other reasons, MetaSwarm may appoint local reputable IT firms as distributors or partnerships to represent MetaSwarm locally. Thus, combining MetaSwarm's international business strategy and the expertise of local business partners to market and sell MetaSwarm's Essurance systems in these areas.
- MetaSwarm will provide overall marketing, sales, and technical support to these distributors/partners to ensure MSWM's products and services have been well represented, and that they serve the customers in the most satisfactory manner possible.
- Revenue Models
- There are several ways for the Company to generate dramatic income from personal information assurance services:
- Validated Advertisements to cellular messaging for SMS/MMS users
- Validated Transaction Services by way of authenticated SMS/MMS messages:
- Banking/ATM
- Credit/Debit Cards
- Brokerage Transactions
- Unsolicited Bulk Message Management for SMS/MMS users
- Monitoring, Filtering, and Message Management Services for SMS/MMS/Internet network providers and oversight groups:
    - MetaSwarm will assist clients in setting up their own AggCenter to support their customers, their websites, and their mailings for a charge, based on number of users and the complexity of their Partner Lists
    - Construction and License fees from government authorities, corporate, local, and/or regional Aggregation Center establishments
    - Services provided to the above Aggregation Centers, such as up-link, backup, etc.

- MetaSwarm will charge the operators of Country and Corporate Aggregation Centers for their center up-link to MSWM's Global Aggregation Center to allow international Internet users to visit their websites and their associates' validated websites, and to receive their and their associates' validated promotional or informative messages.
- Their center will be backed up in real time by a MetaSwarm Global AggCenter for a charge that will provide these operators a peace-of-mind system to focus on their service rather than worry over concerns about their center's stability and reliability.
- Partner List registration fee, globally or regionally
- Additional revenue models will accompany development of future products.

KEY PERSONNEL

MARVIN SHANNON – CO-FOUNDER, CHAIRMAN AND CEO

Marvin Shannon is co-founder, chairman, and CEO of MetaSwarm Corporation. He is co-inventor of over 34 patents pending that provide the basis for the MetaSwarm Essurance system. Mr. Shannon, a 19-year software industry veteran, is a recognized leader in information technology, focusing on technology development and consulting in parallel/distributed computing systems.

Mr. Shannon founded MetaSwarm in January 2003 with a vision to create an effective platform for the uniform management of electronic communications. Under Shannon's direction, MetaSwarm has built a ground-breaking idea into a technology base capable of comprehensively managing email, instant messaging (IM), and cell phone-enabled messaging services (SMS and MMS). His technology enables, for the first time, management of unsolicited bulk advertising (such as spam), and the ability to identify undesirable messages (such as phishing email) and their associated websites.

Previously, Shannon co-founded and was Executive Vice President of planetLingo, Inc., a venture-funded computer-assisted language learning company. He was responsible for day-to-day operations and technology development. Shannon led the creation and release of Internet and CD-ROM language products in Japan and China.

Prior to co-founding planetLingo, Shannon was the Director of Technology and Principal Technology Officer of Citysearch, Inc. Shannon managed the transition from a prototype system to a commercial system serving more than a hundred cities worldwide. Citysearch is now part of Ticketmaster- Citysearch Online, a division of InterActive Corporation.

Shannon studied Physics and Mathematics at the California Institute of Technology.