From: Hallam-Baker, Phillip
Sent: Wednesday, September 29, 2004 9:33 PM
To: Authentication Summit
Subject: E-mail Authentication Summit-Comments

E-mail Authentication Summit Comments
To: Secretary, Federal Trade Commission, Room 159-H (Annex V), 600
Pennsylvania Ave., N.W., Washington, DC 20580
Name: Dr. Phillip Hallam-Baker FBCS, C. Eng.
Position: Principal Scientist, VeriSign
Contact:
1.   Responses relating to IP Address based authentication mechanisms
VeriSign believes that there is a need for two complimentary email
authentication mechanisms, a mechanism that uses the IP address of the
outgoing mail server and a mechanism based on digital signatures. In order
to avoid confusion we answer the questions raised for each technology
approach separately but combine comments on the different proposals that use
the same underlying mechanism.
Although some confusion has recently been created by the closure of the IETF
MARID group without a recommendation to follow a single agreed standard this
state of affairs should be considered temporary. The publication of the
MARID proposals as experimental RFCs will be sufficient to begin large-scale
deployment.
1. Whether any of the proposed authentication standards (either alone or in
conjunction with other existing technologies) would result in a significant
decrease in the amount of spam received by consumers.
The Sender-ID specification based on a merger of the SPF and Caller ID
proposals may be reliably expected to mitigate impersonation spam (also
known as Joe Jobs) and eliminate the use of certain tactics widely adopted
by spammers.
This authentication technology also provides the basis for a medium-term
reduction and long-term elimination of criminal spam when used in
conjunction with third party accreditation and reputation services such as
the VeriSign Verified Domains List (VDL) and the Ironport Bonded Sender
program.
2. Whether any of the proposed authentication standards would require
modification of the current Internet protocols and whether any such
modification would be technologically and practically feasible.
Any authentication mechanism will require certain steps to be taken by both
the sender and the receiver of an authenticated email message. The
modifications required to support the Sender-ID specification are
intentionally chosen to have as little impact as possible on small to medium
sized email senders and an acceptable impact on large and very large email
senders. These modifications are entirely feasible technically and may be
implemented on behalf of end users by a moderately skilled email
administrator without the need for any end-user intervention.
3. Whether any of the proposed authentication standards would function with
the software and hardware currently used by senders and recipients of email
and operators of sending and receiving email servers. If not, what

additional software or hardware would the sender and recipient need, how much it would cost, whether it would be required or optional, and where it would be obtained.

The proposed Sender-ID specification does not require senders to deploy any new software except in the case of the largest email senders where even the smallest change may have significant impact on administration, testing etc. Email recipients that wish to benefit from Sender-ID will need to update their infrastructure accordingly. In most case this will require no more than either a zero cost plug in to work in their existing system or an upgrade to their existing anti-spam solution.

4. How operators of receiving email servers are likely to handle unauthenticated messages.

Unauthenticated messages fall into two distinct categories, those messages that were expected to have authentication but lack it and those from domains that do not support authentication.

It is likely that during the initial deployment phase messages of both types will be subjected to the same spam filtering processes currently widely deployed. As an increasing proportion of email is authenticated the proportion of good mail in the remainder will fall. As a result it is to be expected that email receivers will employ increasingly stringent filtering criteria on the residue of unauthenticated email, progressively raising the discrimination threshold for the spam filtering systems. It is to be anticipated that at some point a significant proportion of senders will begin rejecting unauthenticated email entirely and dispense with their heuristic spam filtering systems.

5. Whether any of the proposed authentication standards could result in email being incorrectly labeled as authenticated or unauthenticated (false negatives and false positives), and the steps that could be taken to limit such occurrences.

There are three possible outcomes from an authentication process, the message can be identified as definitively authentic or definitively fake or the result may be indeterminate, either because there was no authentication information available for the domain or because the authentication process cannot provide a definitive statement for a particular message.

The Sender-ID scheme is only capable of providing either the definitively authentic result or the indeterminate result. Due to the vagaries of email sender configuration it is not possible for Sender-ID to distinguish between a fake message and a message that has been forwarded through a non-compliant server. Judged according to the requirements that Sender-ID sets out to achieve, Sender-ID is unlikely to result in incorrect labeling of messages unless there has been a configuration error by the sending mail administrator.

6. Whether the authentication standards are mutually exclusive or interoperable. Whether any of the proposed authentication standards would integrate with any other standards. For example, if Mail Server is using standard X, will it accept email easily from Mail Server B that is using standard Y?

The Sender-ID scheme is mutually interoperable with and complimentary to the cryptographic mechanisms proposed in MASS. As digital signature schemes inevitably make significant resource demands on the recipient the use of Sender-ID for pre-authentication of mail is highly desirable even in the case that a digital signature scheme is also used.

7. Whether any of the proposed authentication standards would have to be an open standard (i.e., a standard with specifications that are public).

For a specification to provide any value to the community it must be based on an unencumbered open standard and be supported by both the leading vendors of email software and the major ISPs.

8. Whether any of the proposed authentication standards are proprietary and/or patented.

Parts of the Sender-ID standard are subject to pending patent license claims made by Microsoft. Microsoft has however offered a zero royalty license on terms that have on past occasions been considered acceptable for an open

standard.

The SPF, Caller-ID and Sender ID specifications each consists of two parts, a specification that defines a syntax that email senders may use to publish the set of IP addresses of their outgoing edge email servers and rules that define the interpretation of those records.

At the conclusion of the MARID working group agreement had been reached on the use of SPF syntax to achieve the publication of the IP address records and a choice of two mechanisms for interpreting the records.

Although patent claims have been raised with respect to one method of applying the information provided in the DNS records this method is only one means of interpreting the data provided by the sender and the license terms have generally been considered acceptable in the past when offered by other vendors.

9. Whether any of the proposed authentication standards would require the use of goods or services protected by intellectual property laws.

With the exception of the Microsoft patent application mentioned above there are no known intellectual property encumbrances that affect Sender-ID.

10. How any of the proposed authentication standards would treat email forwarding services.

Forwarding services represent the principal source of indeterminate responses when attempting to verify the purported sender using Sender-ID. For this reason forwarding services in particular are strongly encouraged to deploy infrastructure that strictly follows the email protocol standards and preferably adopt Sender-ID authentication in addition.

Even though Sender ID cannot guarantee authentication of the purported sender the specification does allow authentication of a purported responsible address for each message and hence a party that may be held accountable for sending spam.

11. Whether any of the proposed authentication standards would have any implications for mobile users (e.g., users who may be using a laptop computer, an email-enabled mobile phone, or other devices, and who legitimately send email from email addresses that are not administratively connected with their home domain).

Regardless of whether an email sender can establish the authenticity of their reply to address it should always be possible for every email sender to provide at least one domain name for which authentication is possible.

12. Whether any of the proposed authentication standards would have any implications for roving users (i.e., users who are obliged to use a third party submission service when unable to connect to their own submission service).

In principle an email sender could provide support for this type of network configuration by means of appropriately designed authentication records and the use of dynamic DNS.

In practice the normal network configuration is for email messages for roving users to be routed through the mail servers administered by the domain owner and the type of network configuration described is actually rare outside a limited number of communities with very high levels of computer network expertise who may reasonably be expected to adapt to any difficulties caused.

13. Whether any of the proposed authentication standards would affect the use of mailing lists.

The basic Sender-ID standard is compatible with but not optimal for use with mailing lists. The principal issue to be considered when accepting a message from a mailing list is whether the recipient solicited the message or not.

This issue is readily solved by a proposed modification to the mechanism commonly used to authenticate subscription requests in order to create a verifiable proof that the recipient consented to receive the message.

14. Whether any of the proposed authentication standards would have any implications for outsourced email services.

Sender ID is designed to allow the use of an outsourced mail service. This may be for all mail sent from the domain as is common in the case of small enterprises or for selected parts of the mail sent such as bulk email

distributions.

15. Whether any of the proposed authentication standards would have an impact on multiple apparent responsible identities (e.g., in cases where users send email using their Internet Service Provider's SMTP network but have their primary email account elsewhere).

The key issue is whether there is a party who is to be held accountable for sending the email should it turn out to be spam. Sender-ID does achieve this requirement in the context specified.

16. Whether any of the proposed authentication standards would have an impact on web-generated email.

Web hosted email accounts such as that provided by Yahoo, Hotmail and similar providers would not be required to make significant changes in their practices.

Web mail providers that do not perform authentication of the purported sender such as so-called postcard sites will have to make technical changes correctly represent their messages as having been sent on behalf of the purported sender.

This requirement is an inescapable consequence of authenticating the email sender. It is not possible for email authentication to be meaningful to end-users and at the same time support sites that allow anonymous parties postcards that purport to have been sent by anyone the sender chooses.

17. Whether the proposed authentication standards are scalable. Whether the standards are computationally difficult such that scaling over a certain limit becomes technologically impractical. Whether the standards are monetarily expensive due to hardware and resource issues so that scaling over a certain limit becomes impractical.

Sender ID does not entail intensive infrastructure and is entirely practical if deployed on any scale including ubiquitous deployment.

18. Identify any costs that would arise as a result of implementing any of the proposed authentication standards, and identify who most likely would bear these costs (e.g., large ISPs, small ISPs, consumers, or email marketers).

In order to implement the Sender Id specification all a sender need do is to identify the IP addresses of all their outgoing email servers. It is unlikely that this will prove a significant administrative burden for any well run ISP except for the very largest and most complex.

If senders are required to provide accreditation credentials in addition to the IP address authentication credentials then it should be expected that these would cost no more than is currently charged for similar credentials issued for Web site SSL certificates, i.e. in the region of $100 to $1,000 per domain.

19. Whether ISPs that do not participate in an authentication regime would face any challenges providing email services. If so, what types of challenges these ISPs would face and whether these challenges would in any way prevent them from continuing to be able to provide email services.

ISPs who do not participate in the authentication regime should anticipate increasing difficulty in getting other ISPs to accept their email.

This should not be considered a hardship since ISPs are already being faced with a considerable burden when trying to get other ISPs to accept their email. The cost and trouble incurred in deploying Sender Id and appropriate accreditation is significantly less than the burdens currently imposed by self appointed 'block list' vigilantes.

20. Whether an Internet-wide authentication system could be adopted within a reasonable amount of time. Description of industry and standard setting efforts, whether there is an implementation schedule in place and, if so, the time frames of the implementation schedule.

The deployment of an Internet-wide authentication system has already begun and is likely to pick up considerable momentum once the MARID group approves Sender ID as a committee recommendation.

The participation of all the major ISPs, email service providers and spam filtering companies is anticipated before the end of 2005 Q2.

We anticipate that the spammers will respond to the initial deployment of

Sender Id by adopting 'disposable domains', domain names registered for the sole purpose of sending spam and then dropped as soon as they attract a negative reputation. This tactic will in turn lead to email recipients demanding that senders provide accreditation.

It is likely that the adoption of accreditation services will trail the adoption of Sender Id by 12 months. Although many email senders will discover that they already have a form of accreditation through their inclusion in the VeriSign VDL accreditation list compiled from VeriSign certificate holders. The VDL provides a means by which accreditation may readily gain critical mass.

21. Whether any of the authentication standards would delay current email transmission times, burden current computer mechanisms, or otherwise adversely affect the ease of email use by consumers.

After careful analysis of numerous predictions that Sender Id may cause the imminent collapse of the Internet we see no reason to consider these predictions either credible or likely.

22. Whether any of the proposed authentication standards would impact the ability of consumers to engage in anonymous political speech.

We believe that Sender Id encourages free speech. Sender Id prevents one party impersonating another, stealing their reputation and good name. Sender Id does not prevent any party from speaking either anonymously or pseudonymously. Sender Id does however provide a means by which a recipient may choose to reject such messages.

Sender Id operates at the domain name level, not the email address level. It should be noted that those wanting to engage in anonymous political speech usually use the services of a large Internet service provider rather than registering their own domain names. Since Sender Id performs domain name level authentication the transport of emails is unaffected.

23. Whether any safeguards are necessary to ensure that the adoption of an industry-wide authentication standard does not run afoul of the antitrust laws.

Any authentication mechanism must be unencumbered, be readily adopted by any email sender and permit the use of multiple sources of accreditation data.

It must be possible for any party to set up an accreditation service without central approval or access to privileged resources.

Sender Id meets these criteria.

24. Whether a spammer or hacker could compromise any of the proposed authentication standards by using, for example, zombie drones, spoofing of originating IP addresses, misuse of public/private key cryptography, or other means.

The use of spoofed IP addresses is possible but highly unlikely. Spam is almost by definition a mass phenomenon. It is highly unlikely that a spammer could perform this type of attack on a sufficiently large scale to be profitable without being caught.

The lack of authentication in the BGP protocol may provide a vulnerability that some spammers attempt to exploit. Should this prove to be a realistic threat it is an issue that requires urgent attention regardless of whether Sender Id is deployed or not.

25. Whether any of the proposed authentication systems would prevent "phishing," a form of online identity theft.

Sender Id does not provide authentication of the purported email sender address. It is therefore an unsatisfactory solution to the phishing problem but does provide some short-term tactical advantages while a cryptographic approach such as MASS is developed.

26. Whether the operators of small ISPs and business owners would have the technical capacity to use any of the proposed authentication standards. Whether any of the authentication standards could be reasonably implemented by smaller ISPs.

Sender Id can reasonably be implemented by any ISP regardless of size.

27. Whether any of the proposed authentication standards would have cross-border implications.

This issue is not believed to be applicable to Sender ID.

28. Whether any of the proposed authentication standards would require an international civil cryptographic standard or other internationally adopted standard and, if so, the implications of this requirement.
Not applicable.
29. Description of how the Email Authentication Summit can support industry or standard-setting efforts.
Ideally the summit would result in leading industry partners making a public endorsement of an email authentication roadmap in which the first step is ubiquitous deployment of Sender Id and associated accreditation services and the second step is the deployment of cryptographic authentication services by all parties that have a trust relationship with their email correspondents.
30. Assuming a domain-level authentication system is established in the near term, future measures that the private market should develop and implement in order to combat spam.
The primary additional measure required is the development of public accreditation and reputation services as described in this memo.
In addition a number of supporting technologies should be developed to address the 'corner cases' such as mailing lists and forwarding relationships that are not directly addressed in the Sender ID model
2.   Responses relating to Cryptographic Authentication Mechanisms
VeriSign believes that there is a need for two complimentary email authentication mechanisms, a mechanism that uses the IP address of the outgoing mail server and a mechanism based on digital signatures. In order to avoid confusion we answer the questions raised for each technology separately.
Although there is at present no standards proposal for a digital signature based authentication mechanism the IETF MASS working group has been proposed to create one. These answers relate to the MASS working group proposal and in most cases are also applicable to the Domain Keys proposal except where stated.
1. Whether any of the proposed authentication standards (either alone or in conjunction with other existing technologies) would result in a significant decrease in the amount of spam received by consumers.
The MASS proposal is unlikely to be a significant advantage in defeating spam due to the significant length of time required to develop and deploy robust cryptographic authentication mechanisms.
2. Whether any of the proposed authentication standards would require modification of the current Internet protocols and whether any such modification would be technologically and practically feasible.
The MASS proposal will require email senders and recipients to adhere more closely to the email protocol standards than has been the case to date. The proposal is otherwise entirely based on well-understood technologies and there is a very high degree of confidence that it is practical in the cryptographic protocol development community.
3. Whether any of the proposed authentication standards would function with the software and hardware currently used by senders and recipients of email and operators of sending and receiving email servers. If not, what additional software or hardware would the sender and recipient need, how much it would cost, whether it would be required or optional, and where it would be obtained.
Cryptographic authentication such as proposed in MASS and Domain Keys will require a significant software deployment by email senders and in the case of large senders the deployment of a significant infrastructure to sign every outgoing message. It is likely that this requirement will limit the initial deployment of MASS to the owners of major brands such as those targeted in phishing attacks.
4. How operators of receiving email servers are likely to handle unauthenticated messages.
The general consensus is that a mail message that fails authentication for any reason should be treated as if no authentication were provided. This means that in general a recipient should see no warning whatsoever if a

message fails a signature validation test unless the receiving mail agent has a reason to have expected the authentication to be provided.

If the sender of an email message identifies themselves as a likely target of phishing attack and that in consequence of this all outgoing messages are authenticated by signature it is likely that unsigned messages will be discarded in most consumer facing applications.

5. Whether any of the proposed authentication standards could result in email being incorrectly labeled as authenticated or unauthenticated (false negatives and false positives), and the steps that could be taken to limit such occurrences.

There are three possible outcomes from an authentication process, the message can be identified as definitively authentic or definitively fake or the result may be indeterminate, either because there was no authentication information available for the domain or because the authentication process cannot provide a definitive statement for a particular message.

The MASS specification is capable of providing the outcomes definitely authentic, definitely fake or indeterminate due to lack of authentication data for the domain. One of the disadvantages of digital signatures is that they are fragile; a small change to the signed message can invalidate the signature irrecoverably. Accordingly it is to be expected that a proportion of messages identified as definitively fake will be false positives.

6. Whether the authentication standards are mutually exclusive or interoperable. Whether any of the proposed authentication standards would integrate with any other standards. For example, if Mail Server is using standard X, will it accept email easily from Mail Server B that is using standard Y?

The MASS proposal is complimentary to Sender Id and does not raise interoperability concerns.

7. Whether any of the proposed authentication standards would have to be an open standard (i.e., a standard with specifications that are public).

[Same as SID response]

8. Whether any of the proposed authentication standards are proprietary and/or patented.

This statement cannot be answered until the proposal is known in greater detail. It is unlikely that an encumbered proposal would find market acceptance.

9. Whether any of the proposed authentication standards would require the use of goods or services protected by intellectual property laws.

See above.

10. How any of the proposed authentication standards would treat email forwarding services.

Signature based solutions are in principle compatible with email forwarding services provided that the forwarding service does not modify or mangle the forwarded data. It is likely that some such forwarding services would give rise to false positive results.

11. Whether any of the proposed authentication standards would have any implications for mobile users (e.g., users who may be using a laptop computer, an email-enabled mobile phone, or other devices, and who legitimately send email from email addresses that are not administratively connected with their home domain)

[Same as SID response]

12. Whether any of the proposed authentication standards would have any implications for roving users (i.e., users who are obliged to use a third-party submission service when unable to connect to their own submission service).

[Same as SID response]

13. Whether any of the proposed authentication standards would affect the use of mailing lists.

[Same as SID response]

14. Whether any of the proposed authentication standards would have any implications for outsourced email services.

In principle the use of digital signatures could provide greater flexibility

in addressing this issue.

15. Whether any of the proposed authentication standards would have an impact on multiple apparent responsible identities (e.g., in cases where users send email using their Internet Service Provider's SMTP network but have their primary email account elsewhere).

In principle the use of digital signatures could provide greater flexibility in addressing this issue.

16. Whether any of the proposed authentication standards would have an impact on web-generated email.

[Same as SID response]

17. Whether the proposed authentication standards are scalable. Whether the standards are computationally difficult such that scaling over a certain limit becomes technologically impractical. Whether the standards are monetarily expensive due to hardware and resource issues so that scaling over a certain limit becomes impractical.

No difficulties are anticipated in this regard. Although large email senders and receivers will require the capability of generating or verifying large numbers of signatures per second this is readily addressed by commodity hardware acceleration products.

18. Identify any costs that would arise as a result of implementing any of the proposed authentication standards, and identify who most likely would bear these costs (e.g., large ISPs, small ISPs, consumers, or email marketers).

Although small senders could in principle adopt MASS at negligible cost it is most likely that initial deployments will be large-scale efforts by major brands targeted by phishing attacks where cost is a secondary issue. The cost of ordinary certificates for use with MASS would be likely to be in the same order as SSL web site certificates, i.e. $100 to $1000 per server. Certificates with embedded logotype extensions are likely to attract a premium.

19. Whether ISPs that do not participate in an authentication regime would face any challenges providing email services. If so, what types of challenges these ISPs would face and whether these challenges would in any way prevent them from continuing to be able to provide email services

The MASS authentication scheme is likely to be seen as a premium authentication service whose use is restricted to those with a need to establish trusted bona fides with the email recipient rather than a ubiquitous scheme, let alone a mandatory one.

20. Whether an Internet-wide authentication system could be adopted within a reasonable amount of time. Description of industry and standard setting efforts, whether there is an implementation schedule in place and, if so, the time frames of the implementation schedule.

The MASS proposal is considerably less mature than Sender ID and has a much greater impact on the parties responsible for deployment. No implementation schedule is currently agreed in the industry although trial deployment of Domain Keys is proceeding.

21. Whether any of the authentication standards would delay current email transmission times, burden current computer mechanisms, or otherwise adversely affect the ease of email use by consumers

The processing overhead of generating and verifying signatures is unlikely to have a significant on any party being considerably less than is presently performed for spam detection. Ease of use and simplicity is the principle reason why a new protocol is being proposed instead of the reuse of an existing protocol such as S/MIME or PGP. These older protocols offer very high levels of security but are aimed at the technically astute. Most implementations are not appropriate for use by the masses.

22. Whether any of the proposed authentication standards would impact the ability of consumers to engage in anonymous political speech.

[Same as SID response]

23. Whether any safeguards are necessary to ensure that the adoption of an industry-wide authentication standard does not run afoul of the antitrust laws.

[Same as SID response]

24. Whether a spammer or hacker could compromise any of the proposed authentication standards by using, for example, zombie drones, spoofing of originating IP addresses, misuse of public/private key cryptography, or other means.

It is unlikely that any attack of this type would prove feasible.

25. Whether any of the proposed authentication systems would prevent "phishing," a form of online identity theft.

MASS provides a strong proof that an email was generated by the purported sender and may be linked to a conspicuous proof of authenticity. For example a national bank might send out emails that cause the logo of the bank to appear in a privileged portion of an email client or play a relevant jingle.

26. Whether the operators of small ISPs and business owners would have the technical capacity to use any of the proposed authentication standards. Whether any of the authentication standards could be reasonably implemented by smaller ISPs.

The deployment of MASS by a small scale ISP is entirely feasible. We anticipate support for the standard through a number of low cost strategies including low cost appliance style boxes and outsourced services.

27. Whether any of the proposed authentication standards would have cross-border implications.

Although the use of cryptography is restricted in some countries few have restrictions that relate to use of cryptography for authentication. The status of the digital signatures created must be clearly understood to be proof of origin rather than proof of intent to execute a contract or other purpose generally considered under national digital signature laws.

28. Whether any of the proposed authentication standards would require an international civil cryptographic standard or other internationally adopted standard and, if so, the implications of this requirement.

The MASS authentication mechanism does require a new cryptographic standard and development. As a result deployment of this standard will be considerably slower than for Sender Id. In the longer term however it is to be expected that most email senders will transition to using the cryptographic mechanism because of the superior security it provides and also because of the better opportunity for branding.

29. Description of how the Email Authentication Summit can support industry or standard-setting efforts.

[Same as SID response]

30. Assuming a domain-level authentication system is established in the near term, future measures that the private market should develop and implement in order to combat spam.

[Same as SID response]

3.   Additional Information

We believe the following points to be salient even though they are not a direct response to the FTC/NIST questionnaire.

Civil Law

Civil law can act as an effective compliment to authentication technology in addition to accreditation mechanisms. Spammers routinely violate numerous civil and criminal laws, including in many cases court injunctions prohibiting sending spam to one or more ISPs. Although ISPs have been successful in a large number of civil cases brought against spammers the threat of litigation is not yet considered an effective deterrent by spammers.

One of the chief difficulties faced by litigators is identifying the party responsible for the spam. It is likely that domain level authentication technology will significantly increase the deterrent power of civil litigation by making spammers understand that their risk of being caught is very high.

A key objective of any accreditation mechanism should be to obtain an address at which legal process may be served on the accredited party. Obtaining and authenticating such an address is likely to provide a very significant degree of assurance that the party will not send spam in a

manner that is likely to result in significant civil liabilities.

Law Enforcement

Spam is increasingly becoming an enabler of Internet crimes ranging from consumer fraud to complex identity theft. Although law enforcement action should not be considered a substitute for competent technology an investment in deterrent strategies such as law enforcement can significantly increase the effectiveness of technology controls.

Phishing and Carding Schemes

When dealing with Internet crime it is important to deal with the entire criminal enterprise rather than just the most visible aspects of it. Phishing gains considerable attention because large numbers of Internet users have received clearly fraudulent solicitations attempting to obtain their credit card credentials. But phishing crime is only one part of a criminal value chain that has no point without the ability to convert stolen credit card numbers into cash.

Carding, the conversion of a stolen credit card number into cash or fenceable goods is the other half of the phishing value chain. Traditionally carding has been the hardest and riskiest part of the process since the perpetrator must evade the sophisticated fraud prevention controls of the card companies.

It is likely that the recent increase in phishing activity reflects recent criminal innovation in the area of carding in particular the spread of 'package reshipping' schemes. In a package reshipping scheme the carding gang recruits the gullible or criminally inclined through bogus employment as a 'delivery specialist' or 'finance director'. In the package-reshipping variant of the scheme the carding gang buys fenceable goods such as expensive cameras using a stolen credit card and gives the address of a recruit working in the US as the delivery address. The recruit receives goods bought with a stolen credit card and reships them abroad to the carding gang in return for a commission. The purpose of the recruit for the is twofold, first to evade the fraud controls of the credit card companies and secondly to face the consequences once the scheme is discovered by law enforcement.

Recruitment to 'work at home' schemes of this type is likely to be significantly reduced if a publicity campaign convinced a sufficiently large fraction of the public that participation in these schemes is 1) criminal 2) inevitably going to be discovered and prosecuted.