GLOBAL WORKSPACE ASSOCIATION

Virtual Office 'Best Practices' Guidelines

Providers of workspace-as-a-service allow a growing number of professional businesses to succeed by providing them with a variety of physical and virtual workspace solutions. In the past, the industry has come under scrutiny by law enforcement agencies as well as corporate fraud prevention professionals for representing a potential medium for fraudulent activity. As providers of workspace-as-a-service, we have an important role to play in protecting the public, the industry and our own businesses from being harmed or discredited by association with even one client's fraudulent practices.

The Global Workspace Association (GWA) recommends that you provide a copy of this handout to each of your company's employees to use as a reference tool. It is designed to help each of you be good stewards of our industry and its future.

Best Practices for Vetting Virtual Office Clients

as Recommended by the Global Workspace Association

- Ensure that each location you operate is registered as a Commercial Mail Receiving Agency by filing a USPS 1583a with the local post office
  - For more information go to http://www.usps.com and search "CMRA".
  - For forms to register your center: http://about.usps.com/forms/ps1583a.pdf or
  - Forms for your prospective clients to complete http://about.usps.com/forms/ps1583.pdf

  Note: The GWA encourages all office business centers, even those whose virtual office programs are exempt from compliance, to require their clients to complete Form 1583 for, at least, for its fraud prevention benefit. Enforcement of CMRA regulations varies greatly among postal districts. To determine if your center requires CMRA compliance or if you meet the standards for exemption, go to: http://pe.usps.gov/text/dmm300/508.htm

  For International Operators – please ensure that you are educated about your country's specific requirements regarding mail forwarding, legal requirements and other regulatory restrictions.

- Before you propose services to a virtual prospect, perform an internet search on the company name and the client name.
- Other suggested research sites include:
  - www.BBB.org
  - www.DnB.com
  - www.RipOffReport.com
  - www.Complaints.com
  - US Securities and Exchange Commission Brokers Central Registration Depository www.SEC.gov/investor/brokers
  - Other resources to access are *profession based* such as your state's Bar Association, or Department of Real Estate, or other professional state based or national associations.

Virtual Office 'Best Practices' Guidelines

- Before commencing mail-handling services for any virtual client, obtain properly completed and, if applicant is not in your presence, fully notarized CMRA form USPS1-A for each company and individual for which mail will be received.
- New web based or digital tools such as online notary services and business information verification databases may provide additional fraud prevention screening while providing customer convenience.

  For International Operators – please search your country's appropriate resources to inquire about an entity's business rating, credit rating, on-line complaints, etc.

- Google the IP address where the inquiry came from and note the server address. Be wary of inquiries from individuals overseas.
- Often times individuals engaged in scams will access the internet from various locations as they are trying to mask their physical location. Ongoing logging/monitoring of the originating IP addresses of email received from prospects / clients is a good practice. Taking the time to learn how to analyze email headers and originating IP addresses can be very productive toward determining ~~potential~~ a potential fraud or scam. Here is a good basic introduction: http://www.ehow.com/how_6592820_read-email-header-information.html
- Review and screen all documents and required sources of identification carefully for discrepancies. The CMRA Form requires 2 forms of identification - one of which must contain a photograph and both must have a home address that match. Acceptable identification includes: valid driver's license or state non-driver's identification card, armed forces identification, passport, alien registration card or certificate of naturalization; current lease, Mortgage or Deed of Trust, voter or vehicle registration card, or home or vehicle insurance policy. Most clients use their driver's license and their vehicle registration card.

- Review signatures – Do they match? You are checking if one may be forged. Are they too perfectly matched? This would suggest they might be copies
- Review documents for signs that something is amiss. The "cut and paste" method is a common way to forge or falsify documents.
- If a client shows up on a D&B report, check details: Is the potential client the same type of business, in the same city, have the same number of stated employees? If not, applicant could be a stolen or fraudulent business identity.
- Call all listed telephone numbers and test URL's
- Consider requiring a credit check on each new client.
- Consistently gather data such as social security numbers and driver's license numbers to keep on file.
- Do not allow payment in cash or due more diligence if credit card is in someone else's name. Be wary of credit cards from overseas.

- Watch for 'suspicious' mail or activity. Pay careful attention to clients asking for mail or packages to be forwarded internationally, this is a common ploy for fraud.
- Monitor user names and company names carefully. Name changes for existing clients should be as scrutinized as applicants.
- Consider participation in community crime fighting efforts such as the FBI's InfraGard, a public-private resource sharing program to help stay current of criminal trends. (www.InfraGard.net)

Most importantly...BE AWARE and USE COMMON SENSE. If something "feels" wrong, expand your due diligence.

Understanding the Potential for Fraud When 'Best Practices' are not Followed

The following 'case studies' are real life illustrations

Re-Shipping Scams

A center signed up a new virtual mail service client who provided all required documents (license, passport, etc.), and presented a credit card for payment. He provided the center with prepaid UPS labels and requested that packages received for the business be re-shipped using the labels. The credit card was declined, and the client presented another card, which was also declined, but packages were already starting to arrive. Shortly after the second credit card decline notification, the police visited the center and confiscated all of the packages that had arrived for the client, declaring them stolen property. The center learned that the credit cards and identities were stolen. The address the client had given for re-shipping belonged to someone who did not know of the scheme, but lived in an apartment where packages were delivered and left unsecured in the lobby. The client would case the lobby and pick up the packages before they were seen by the apartment manager.

> ***Don't be the victim of a reshipping scam! This Postal Inspectors website gives more details about how these scams work:*** https://postalinspectors.uspis.gov/radDocs/consumer/ReshippingScam.html

E-Commerce Fraud

A prospect walked into a center inquiring about mail services. After expressing interest in a mail account he received an Agreement, promising to return the next day to finalize the paperwork and provide opening funds. He was not heard from for about a week. When packages from a merchant began to arrive for him, the Center Manager called to inquire about his agreement. With further promises, she allowed him to pick up the packages letting him know that he would need to complete the paperwork and remit funds before using the mailing services again, which he did. A few months later, however, the merchant contacted the center to let them know that the client was committing fraud by ordering goods and taking receipt of products with no intent to pay, which a crime. Thwarting this criminal's efforts on the front end might have been possible by refusing to take delivery of packages prior to having the Agreement and all supporting documents in place.

> ***Never provide ANY package handling services to any client with whom you do not have a written agreement.***

For more information on e-commerce fraud scams, visit the Merchant Risk Council website at www.merchantriskcouncil.org . Non members can access PDF articles through the site's Press Room

E-Commerce Fraud – International Clients

A center found itself in the middle of an overseas fraud by signing up a mail service client who inquired by email. The center received a signed agreement and a credit card in the name of Lisa F_, but the CMRA documents were not returned. The card was charged and soon a package arrived. The client requested the package be forwarded to Japan. A few days later an online vendor in the US contacted the center asking if they were aware that this company was using the center's mailing address to commit fraud. By that time, the center was already questioning this client and subsequently found the following information – The permanent address given for the client was in East Java, Indonesia and the address entered for the credit card was returned by the credit card processing service as "no match." The center learned that the credit card had been stolen. The center discontinued services immediately, reversed the credit card charges and learned some valuable lessons.

It is important to double check all client information prior to initiating service, looking for inconsistencies and errors in all information provided by the client. Remember, it is okay to go back to the client and ask for clarification – this shows the honest client that you are careful about your due diligence.

The FBI monitors a group called IC3 which was established in partnership with the FBI to research, monitor and aggregate online fraud complaints along with assisting with law enforcement activities. The Press Room of the following site can provide information regarding scams, potentially some from 'high risk' countries **http://www.ic3.gov/default.aspx**

Relay Call Fraud

A center received a call from a deaf relay operator to inquire about virtual office services. The deaf relay service is a Federally- funded program to allow hearing impaired individuals to make and receive phone calls. The hearing impaired individual types communication on a special machine and the relay operator places the phone call and types the caller's response back. The center closed the virtual office package and charged the credit card provided. A day or two later a large box was delivered through the relay operator instructions were given to forward the package to Nigeria.

The center forwarded a few more of these packages then received a "off the record" communication from the relay operator telling them that the caller they were communicating with was a criminal. Shortly thereafter the credit card company reversed the payments as they discovered that the card used was stolen. The center subsequently learned that deaf relay calls can be a tool for criminals because Federal Law actually prohibits the relay operators to interfere or intervene in any relay conversation.

Be wary of customers with whom you never personally speak. For more information on relay fraud go to www.fcc.gov/guides/ip-relay-fraud

If You Suspect Fraud – Who Do You Contact

Certainly, each case will be different and your suspicions will be your guide. However, following are some recommendations:

- Local law enforcement
- State of Local Compliance Agencies: Department of Real Estate, Department of Insurance, Boards of Contractors, etc.
- Department of Homeland Security www.ICE.GOV/TipLine or 866.DHS.2.ICE
- Your local post office or United States Postal Inspection Service www.postalinspectors.uspis.gov
- Federal Trade Commission www.FTC.gov
- Regional Consulate or Embassy personnel

What to when a 'Policing Agency' contacts your center?

The GWA recommends that member companies provide requested assistance to all government policing agencies and to officers that submit proper identification.

The FBI recommends the following procedures to ensure you provide information only to a legitimate inquiry: 1) require the representative requesting information visit your office, 2) copy down the "agents" badge or credential information and request the "main office" number of the agency, and 3) excuse yourself to contact the number and verify badge number as well as the visit.

Remember, these agency representatives work for you and the public. They should be more than happy to provide this information to anyone who inquires.

How can GWA help?

The Global Workspace Association is committed to helping its membership follow best practices and averting fraudulent activity. All members are invited to pay special attention to *Space Matters* where the association will share research and trends in criminal activity. The Association will also coordinate periodic webinars designed to train members and their employees.

Show the world that your company follows the Global Workspace Association's *Virtual Office 'Best Practices' Guidelines by* signing the Pledge and showcase your company's commitment with the "Fraud Watch" seal

The GWA created a visual representation of the membership's commitment to following best practice client vetting techniques. Every GWA member that commits to following these guidelines to the best of their ability will be granted the use of the GWA's 'Fraud Watch' seal. By signing a simple Pledge, drafted by the GWA you will make this commitment on behalf of your clients, your business and your community of Workspace providers.

Proudly display this seal to your clients and prospects to give them the assurance that the very best efforts are made to protect the integrity of the address under which they represent their own business, and to know that the individuals with whom they share space / services have undergone a protective level of vetting. Most

importantly, use your 'Fraud Watch' seal to let fraudsters, who hope to find a service provider that will look the other way, know that fraud will not be tolerated in your location and they need not inquire.

For a copy of the Pledge contact any GWA staff or Board Member.

Virtual Office 'Best Practices' Guidelines

GWA Virtual Offices Pledge to 'Best Practices'

I, _____ (owner, operator or manager) pledge to follow the Global Workspace Association's Best Practices Guidelines to the best of my ability.

Best Practices are as follows:

- I will recommend that each of my workspace locations is in full compliance with the Commercial Mail Receiving Agency requirements as outlined by the USPS.
- I will perform basic due diligence on prospective clients via the internet by researching the company name and each individual prospect name.
- Before commencing mail handling services for any virtual client, I will obtain properly completed and, if applicant is not in my presence, fully notarized CMRA Form USPS1583 for each company and individual for which mail will be received.
- I will review and screen all documents and required sources of identification carefully for discrepancies.
- I will call listed telephone numbers and test URL's
- I will not allow payment in cash and will verify credit cards in someone else's name. I will be wary of credit cards from overseas.
- I will watch for 'suspicious' mail or activity and will pay careful attention to clients asking for mail or packages to be forwarded internationally
- I will monitor user names and company names carefully. I will also scrutinize the name changes of existing clients as closely and I do applicants.
- I will be aware of my client's activities and I will be on the lookout for unusual activity.
- I commit to following the GWA's Code of Ethics found at http://www.globalworkspace.org/documents/code_of_ethics.pdf

By signing and dating below your company will be given access to proudly display the GWA's 'Fraud Watch' Seal which will give your prospects and clients the confidence to know that fraud protection efforts will be followed to the best of your ability.

_____ _____

Name Date

_____

Title

_____

Company Name

For International Operators – please ensure that you are educated about your country's specific requirements regarding mail forwarding, legal requirements and other regulatory restrictions.