



## Warning – Fraudulent Emails

This document provides information to users of IATA products and services (e.g. airlines, agents, other companies and individuals) so that they may avoid becoming a victim of **email fraud attempts**. Please read this information carefully and share it with your colleagues.

*(double click the icons below to navigate)*



**Read about email fraud techniques**



**Examples of fraudulent emails**



**Learn how to protect your company**



**Report a possible fraud**

If you have any questions concerning this document, kindly send your queries to:  
[information.security@iata.org](mailto:information.security@iata.org)



## Read about email fraud techniques

Many types of fraud exist, and email is an inexpensive and popular method for distributing fraudulent messages to potential victims.

Some of the most common fraudulent messages are non-monetary hoaxes or non-monetary chain mail. Treat these as you would any other spam. However, if you receive an email message that appears to involve payments, or asks for personal information, do not respond.

**Several attempts have been made to obtain payments from users of IATA products and services. The most common technique is through the use of fraudulent emails.**

The methods employed generally include elements of the following:

1. **The fraudster contacts users under a false name**, sometimes similar or identical to the names of IATA officials, seeking payment for products or services and/or claiming payments for outstanding amounts due.
2. **The fraudster uses an email address resembling IATA** email addresses but using different host servers.

### Recent examples:

[account@iataacc.org](mailto:account@iataacc.org)

[account@iata-payment.org](mailto:account@iata-payment.org)

[account@iatamgt.org](mailto:account@iatamgt.org)

[billing@iataservices.org](mailto:billing@iataservices.org)

[credit@iata-payment.org](mailto:credit@iata-payment.org)

[payment@iata-billing.com](mailto:payment@iata-billing.com)

[account@iata-online.org](mailto:account@iata-online.org)

[iatatr@yahogroups.com](mailto:iatatr@yahogroups.com)

[user@iataworldwide.org](mailto:user@iataworldwide.org)

[invoice@iata-payments.com](mailto:invoice@iata-payments.com)

3. **The fraudster uses a technique which allows the name of the sender of an email to be doctored and masked**, so that the email appears to have been sent from a valid IATA address like [finance@iata.org](mailto:finance@iata.org).
4. **The fraudster uses forged documents** bearing the official IATA logo, most likely copied from our website.



5. **The fraudster's email may suggest clicking on a link.** After clicking on the link, the user is taken to a bogus website that requests your login details, the purpose of which is to steal your login credentials.

Some attempts are presented **to appear as though they originate from a '@iata.org' address**, although this is simply a mask and the address is not valid. In such cases, the fraudster asks the recipient to reply to another email address, such as a "gmail" one.

**The names of IATA employees in the email signatures** have most likely been obtained when recipients of the first email have provided copies of correspondence with IATA. **In some cases, the phone numbers have been changed to invalid numbers**, a tactic most likely designed to prevent the recipient from contacting the sender by phone.

**Typically, the first contact is a generic email** designed to elicit a response from the recipient. If the recipient engages with the fraudsters, they then provide a more detailed request, using language most likely copied from our website.

**Sometimes, this is accompanied by a fraudulent invoice.** The invoice appears at times to be based on a genuine IATA or Strategic Partner invoice.

The fraudster has been able to make these look reasonably authentic as some recipients of the first email have queried the existence of outstanding amounts and provided the fraudster with a copy of a genuine invoice that had already been paid, this provides the fraudster with an appropriate invoice style and content.

Fraudulent invoices in the past have included charges relating to IATA Ground Handling Council membership fees, designator fees, and prefix code retainer/administration fees.

**Fraudulent emails may also include a link that takes the user to a spoofed (fake) IATA website.** The purpose of spoofing an IATA website is to mislead the user into believing he is logging on to a legitimate IATA website.

Once the login details are captured, the fraudster can then use the information to login as the user to obtain billing information that will add authenticity to the fraudulent email attempts. You should always log on to an official website, instead of "linking" to it from an unsolicited email.

If you have, or even believe you have inadvertently responded and/or activated any link or attachment within a fraudulent email, please contact [information.security@iata.org](mailto:information.security@iata.org) with the corresponding details.



**The fraudster indicates in the emails that new payment arrangements are in force** and that the payment requested (or simply future payments where the approach is generic in style) should be made to a new bank account.

Bank accounts with the following financial institutions have been used by the fraudster:

<b>Country/Territory</b>	<b>Financial Institution(s)</b>
Bulgaria	DSK Bank
Canada	TD Canada Trust, CIBC, Royal Bank of Canada
Germany	Hamburger Sparkasse, Sparkasse Landsberg-Diessen
Hong Kong	Bank of China (HK) Ltd; Standard Chartered Bank; Citibank; DBS Bank; Hang Seng Bank, HSBC Hong Kong
India	State Bank of India
Indonesia	CIMB Niaga Bank
Netherlands	ING Bank, Rabobank, Van Lanschot Bankiers
Singapore	ANZ Bank; DBS Bank; HSBC Bank; OCBC Bank; Standard Chartered Bank; United Overseas Bank
Taiwan (R.O.C.)	Fubon Commercial Bank; Taiwan Cooperative Bank
United Kingdom	Barclays; Halifax; HSBC; Lloyds TSB; NatWest; Royal Bank of Scotland; Santander Bank
United States	Bank of America; BB&T Bank; Chase Bank; Citibank; First Financial Credit Union; First Keystone; First State Bank; Greater Texas Federal Credit Union; HSBC; JP Morgan Chase Bank; Prosperity Bank; Regions Bank Suntrust Bank; TD Bank; Thumb National Bank; US Bank; Wells Fargo Bank

Officials at these financial institutions have, by and large, cooperated in the past to investigate and/or close accounts reported to them as being used for the purpose of perpetrating fraud.

If you have been the victim of fraud and have transferred funds to a financial institution as a result of responding to a fraudulent email, you should contact your financial institution immediately as well as filing a complaint with local law enforcement.

If you receive a suspicious or potentially fraudulent email, please report the relevant information to the following email address: [information.security@iata.org](mailto:information.security@iata.org).



To add authenticity to the advice of the new banking details, a “Letter of Authorization”, “Notification Letter”, or ‘Important Notice’ is sometimes provided. These advices display varying styles, but all have the IATA logo present. These are likely to have been obtained from documents on the internet, or from copies of documents provided to the fraudster by recipients of the fraudster’s emails, when responding to queries.

**Example:**



Our Ref: IATA/ORG/VOL. 2011

Date: 01/August/2011

ATTN:

**NOTIFICATION LETTER**

We want to use this medium to inform our numerous clients that there is a change in our banking details and further payment should be paid into it and it takes immediate effect. Below is the new banking information;

**STANDARD CHARTERED BANK HK LTD**  
**ADDRESS: 623 NATHAN RD, MONGKOK, KL HK.**  
**SWIFT: SCBLHKHH**  
**ACCOUNT NUMBER: 570-1095-9421**  
**BENEFICIARY: BING GLOBAL CONSULTANT LTD.**  
**ADDRESS: RM 1312 HOLLYWOOD PLAZA,**  
**NATHAN ROAD, MONGKOK, KL, HK.**

Also, as soon as any payment is effected into this account, do kindly send to us receipt of payment for our record purposes. We are sorry for any inconvenience. Please confirm the receipt of this mail. Thank you for your understanding and total cooperation.

Gunther Matschnigg  
Senior Vice President



Thomas Windmuller  
Senior Vice President

800 Place Victoria P.O Box 113. Montreal Quebec - Canada H4Z 1M1  
Canada



For further insight into the techniques deployed by fraudsters, please follow the below link for a recent example:

<http://www.tnooz.com/2013/05/13/news/exposed-how-online-fraudsters-dive-deep-into-iata-processes-to-secure-payments/>



## Read examples of emails

Being able to recognize such emails can help prevent you from becoming a victim. Below are examples of some recent emails received by users of IATA products and services. The following link provides further insight into a recent attempt

### Example No. 1

----- Original Message -----

**From:** [Account Department](mailto:admin@iataaccounts.org)

[mailto:admin@iataaccounts.org]

**Sent:** Sunday, June 20, 2010 3:47 AM

**Subject:** IATA PAYMENT

**Fraudsters have opened domains mimicking IATA email addresses. They are also now spoofing our legitimate .org addresses. However, they still use addresses opened with free internet service providers.**

*Attn: Sirs,*

**Fraudulent emails often begin with a generic greeting such as "Attn: Sirs" or "Dear Client" rather than addressing you by name.**

*Your company is indebted to us in the area of International Air Transport Association for flights operated in our airspace amount 120,433.12Euros.*

*We have stopped using our old Bank due to their delay in receiving our payment so we advice as soon as you update us on our invoices for payment.*

**Some emails will refer to a "problem" with the bank or your account and urge you to make payments to new account. We will never notify you of a problem through an unsolicited email.**



*Kindly take note of our new account details and please update your file.  
We advice you update us now to enable us resolve this payment asap.*

*Brgds,  
Director General*

**There is often a sense of urgency in the email encouraging you to respond immediately and to update your records with a new address, contact name, or bank account.**

## Example No. 2

----- Original Message -----

**From:** [International Air Transport Association](mailto:internationalair.iatatransport@gmail.com)  
[mailto:internationalair.iatatransport@gmail.com]  
**Sent:** Wednesday, February 10, 2010 17:37  
**To:** undisclosed-recipients  
**Subject:** From International Air Transport Association

**Fraudsters use an email account such as gmail.**

*Dear Sir,*

*Your company is debted to us (IATA) check your record file and also kindly renew your membership with us IATA Ground Handling Council membership or we will remove your company name from IATA Ground Handling Council membership.*

*We look forward to read from you soon.*

*Regards,*

*Paul Adams*

*Accountant*

*International Air Transport Association*





## Report a possible fraud

If you receive a suspicious or potentially fraudulent email, please report the relevant information to the following email address: [information.security@iata.org](mailto:information.security@iata.org).

When reporting such messages, it is important to copy and paste the entire email, including the header information.

### **To display full message headers:**

Open the mail message.

- In Outlook 2010: click the message so that it opens in its own window. In the menu above click File, then click Info and then the Properties box.
- In Outlook 2007: double-click the message so that it opens in its own window. In the Options group, click the dialog box launcher (small square with an arrow).
- In Outlook 2003: from the View menu, select Options. The message headers are at the bottom of the window, in a box labeled "Headers:" or "Internet headers:"

### **To insert the headers into an email message:**

Select all the headers by clicking and dragging the cursor from the top left corner to the bottom right corner of the header text. Press Ctrl-c to copy the headers to the Clipboard. Create a new email message, click in its main text window, and press Ctrl-v to paste the headers.

Transmit the email to [information.security@iata.org](mailto:information.security@iata.org).

If you believe you are a victim of email fraud attempt, we recommend that you also contact your local law enforcement authority immediately. Action Fraud UK, IC3 in the United States and the Canadian Anti-Fraud Centre all offer assistance. For other jurisdictions please contact [information.security@iata.org](mailto:information.security@iata.org).





## Learn how to protect your company

**All organizations are vulnerable to fraud**, especially if elements of the following apply:

1. **Belief that fraud doesn't affect your organization.** In truth, businesses around the world lose millions each year to frauds. Many organizations aren't even aware that they have fallen victim to fraud.
2. **Organization does not have set procedures in place** to authorize purchases, pay invoices and review expenditures.
3. **Personnel are distracted** when they pay invoices such that fraudulent emails and invoices escape their notice.
4. **Personnel do not have time to verify** the source of the email requesting payment. To resolve the matter, the invoice is paid out of convenience without further investigation.
5. **Organization experiences regular staffing changes** related to high turnover, part-time or volunteer staff which increases the risk of falling victim to a fraud.
6. **Personnel recognize the name** and logo of IATA from having paid similar invoices in the past. As a result, they might not review transactions or invoice details before making a payment.
7. **Organization does not report the fraud** because personnel are either embarrassed or ashamed. Law enforcement agencies depend on organizations that have fallen victim to come forward and report fraudulent activity.





## Learn how to protect your company

**Learn how to avoid fraud by reading stories of recent victims.** The following are based on real individuals who have been targeted by fraudsters. To protect individual privacy, the names of people and companies have been omitted.

### Example 1: Fraudulent invoice

Company A received an email from a gmail email address, but apparently from IATA's Director General and CEO, advising them that they were indebted to IATA. It stated that, if they failed to take action, IATA's 'international debt collectors' would visit the company.

The company did not consider the email to be suspicious, even though it was not addressed to them specifically (it had been sent to the Operations Manager's email address listed on the company's website), the language used was threatening, it came from a "gmail" address, and was apparently from the CEO of IATA.

Company A was coincidentally about to renew their membership of the IATA Ground Handling Council (IGHC) and responded to the fraudsters, asking if it related to that. The fraudsters confirmed that it did and sent the company an invoice. The invoice bore the IATA logo (most likely obtained from the internet). The email from the fraudsters referred to a change in bank account and asked the company to make the payment to the account detailed on the invoice. This bank account was in Cyprus.

The company made the payment to the fraudsters' bank account.

When the company received a reminder from IATA about their outstanding IGHC renewal fees, they realized that they had been defrauded.

### Example 2: Change in banking details

Company B received an email from someone who described themselves as a 'Customer Services Representative' informing them that they were indebted to IATA. It stated that, if they failed to take action, IATA's 'international debt collectors' would visit the company.



The email appeared to come from an '@iata.org' email address, but it asked the recipient to respond to another email address because IATA was experiencing problems with its '@iata.org' addresses.

The company did not consider the email to be suspicious, even though it was not addressed to them specifically (it had been sent via the contact us' link on the company's website), the language used was threatening, and it asked for a response to be sent to a non-'@iata.org' email address.

They did not think that they were in debt to IATA, so they responded to the fraudsters, asking for more information.

The fraudsters replied acknowledging that the company was not in fact in debt to IATA, and requested the company to inform them when their next payment was due, as IATA's banking details had changed, due to 'problems with the bank'. The fraudsters said that they would then send the company new banking details.

When the time came to make the next payment, the company notified the fraudsters, who provided account details for IATA's 'subsidiary' to whom payment was to be made.

The company subsequently made their next payment to the fraudster's bank account and did not question the fact that the new account was in a completely unrelated name, and based in China.

IATA's Accounts Receivable department contacted the company in due course to enquire about the payment of their now outstanding debt. The company informed IATA that they had already made the payment to the new bank account 'as requested', and provided confirmation of their payment. At this point, the company realized that they had been defrauded.





## Learn how to protect your company

Here are other **things you can do today** to protect your organization from email fraud:

1. **Don't judge reliability** by look and content. Email messages can come from many sources and with the help of today's technology a fraudster can make an email and invoices appear to be coming from a reputable source.
2. **Review all invoices** and charges regularly.
3. **Be wary of requests** to "update" bank account information or to pay overdue invoices as you may be providing criminals with the information they need to gain access to others in your organization or to defraud third parties.
4. **Implement a policy of checking**, and having independent approval of, any changes to existing, or setting up any new, payee bank account details.
5. **Assign a limited number** of employees to make purchases. Make sure that employees with financial signing authority understand what responsibilities are tied to signing their names on invoices and purchase orders.
6. **Talk to your staff and colleagues about fraud.** Decide how your organization will handle situations involving employees coming forward to report losses.

