

## **Brokers International Financial Services LLC, Security Measures (Recognizing Scams and Identity Theft)**

### **Background**

This information will help answer some of the concerns that you may have around the security of your online transactions.

Brokers International Financial Services (BI Financial Services) makes every effort to enhance the security of your data. Protecting our customers is just good business. Despite all of our efforts, however, there are risks associated with doing business over the internet. You can take some action to protect yourself, and we encourage you to read this information:

#### **1. What is "phishing?"**

A phishing attack is an online fraud technique that involves sending official-looking email messages with return addresses, links and corporate branding that all appear to come from banks, retailers, credit card companies and other legitimate businesses. These emails typically contain a hyperlink to a spoof website. The goal is to mislead account holders to enter confidential information and security details like ID's and passwords on the pretext that some of your information must be updated or changed. Once you provide this information, the cyber criminals can access legitimate sites and steal your money.

It is important that you are suspicious of emails asking for your confidential information. BI Financial Services will never ask you for your personal information by email. This may include your Social Security number, date of birth, bank account number and user name and password.

#### **2. Advanced-fee fraud**

You may already have heard of advanced-fee fraud. In this instance, emails offering the recipients large sums of money are sent to thousands of email addresses. A modest fee is required to cover legal costs, open an account or pay customs' charges. Sometimes, the money offered is the result of a lottery even though you never bought a ticket. Other times, the money is held in an account overseas but the account owner cannot access it. The cyber criminals promise a percentage of the money in return for your help. In both cases, various fees have to be paid right away.

Do not respond to these emails. They are part of a fraud and you will not receive any of the promised money.

#### **3. Verifying Web sites**

Customers can verify that the web site they are entering is secure by following these two guidelines:

The URL will begin with https://

The application window will specify that SSL (Secure Sockets Layer) is in use

## 4. Protecting yourself

### Take care of your personal information

Your account numbers, customer number, PIN number, password and other personal information are the keys to your account. Never write them down, give them to anyone else or include them in an email. Destroy documents containing personal information securely, and be very cautious about posting personal details on social networking sites on the internet. Criminals can use this information to commit fraud. Remember that protecting your personal information is your responsibility.

### Take care of your computer

- Update your computer by installing the latest software and patches to prevent hackers or viruses from exploiting any known weaknesses in your computer.
- Install and update virus protection to protect against viruses corrupting your computer and to prevent hackers from installing Trojan viruses on your computer.
- Install and update anti-spyware tools. (Spyware is computer software that is installed on your computer without your consent to collect various types of personal information or interfere with your computer in various ways).
- Install and update personal firewalls. (A firewall is a hardware or software device that regulates the flow of information between computers).
- Use only programs from a known, trusted supplier.

### Beware of spam emails

Spam emails are messages that are sent simultaneously to thousands of email addresses from an unfamiliar sender.

- Use a spam filter to avoid even seeing these messages.
- Never respond to a spam message, your email address is then recorded as live and the spam will increase.
- Should you read a spam message remember: If it sounds too good to be true, it probably is too good to be true.

## 5. More information

The U.S. Federal Trade Commission provides information on how to avoid phishing scams. Go to [www.ftc.gov/bcp/menus/consumer/tech.shtm](http://www.ftc.gov/bcp/menus/consumer/tech.shtm).

The [Anti-Phishing Working Group](http://www.antiphishing.org) (APWG) provides statistics on phishing attacks and advice for individuals and companies. APWG is a global pan-industrial and law enforcement association focused on eliminating fraud and identity theft that result from phishing and other online scams. Go to [www.antiphishing.org](http://www.antiphishing.org).

## 6. Helpful guidelines

### Helpful guidelines to protect your identity from theft:

- Removing mail from your mailbox every day (or better yet, sign up for electronic statements!).
- Never leaving bills in your mailbox overnight—always put them in a secure US postal mailbox (or better yet, get rid of them and pay bills online!).
- Knowing your billing cycles. Follow up with creditors if bills or new cards don't arrive on time. (An identity thief may have filed a change of address request in your name with the creditor or the post office.)
- Shredding receipts and mail, especially pre-approved credit card applications.
- Eliminating the receipt of pre-approved offers of credit by calling 1-888-5-OPT-OUT.
- Never carrying your Social Security card or bank passwords or other sensitive information in your wallet.
- Accounting for all new checks when you receive them in the mail.
- Removing your name from direct mail lists and writing to the companies you do business with and ask them not to sell or rent your name. You can visit the Direct Marketing Association's website ([www.the-dma.org/](http://www.the-dma.org/)) to learn about the laws that protect you as a consumer and how to get your name removed from these lists.
- Ordering copies of your credit report once a year from one of the three national credit-reporting agencies and looking for accuracy and for indications of fraud, such as unauthorized applications, unfamiliar credit accounts, credit inquiries and defaults and delinquencies that you did not cause.
- Checking your Social Security Earnings and Benefits statement once each year to make sure that no one else is using your Social Security number for employment.

### Be suspicious about telephone calls where:

- The company has a name that is intended to sound like a government agency or a well-known company.
- The company is unwilling to send you written information on the offer or give you references.
- Someone claims you've won a prize and you haven't entered a contest.
- A telemarketer asks for your Social Security number, calling card or credit card number, so you can purchase products or qualify for prizes.
- You have to pay a fee before you receive complimentary goods or services.
- In general things sound too good to be true!

### Bank, shop and spend wisely by:

- Canceling your unused credit cards so that their account numbers will not appear on your credit report.
- Signing your credit cards immediately upon receipt.
- Doing business with companies you know are reputable, particularly online.
- Using a secure browser when you conduct business online that encrypts or scrambles purchase information. (Make sure your browser's padlock or key icon is active.)
- Avoiding opening e-mail from unknown sources.
- Never clicking on an e-mail link. Go to the company's website yourself and fill out information there or call them.
- Asking businesses what their privacy policies are and how they will use your information: Can you choose to keep it confidential? Do they restrict access to data?

## **Helpful guidelines if your identity has been stolen:**

### **1. Contact your bank(s) and credit card issuer(s) immediately to:**

- Protect the access to your accounts.
- Stop payments on missing checks.
- Change personal identification numbers (PINs) and online banking passwords.
- Open a new account if appropriate.

### **2. File a report with your local police department and:**

- Obtain a police report number with the date, time, police department, location and name of the police officer taking the report.
- Agree to an investigation (if the police recommend it) into the loss. The police report will be helpful when clarifying to creditors that you are a victim of identity theft. Complete an Identity Theft Affidavit form and submit it to the appropriate companies. You can download a copy of this form at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft).

### **3. Contact the three major credit bureaus and request a copy of your credit report and:**

- Review your reports to make sure additional fraudulent accounts have not been opened in your name or unauthorized changes made to your existing accounts.
- Request the "inquiries" be removed from your report from the companies that opened the fraudulent accounts. Here are the major credit bureaus and their phone numbers: Trans Union 1-800-680-7289, Experian 1-888-397-3742 and Equifax 1-800-525-6285. You may also contact the FTC's ID Theft Consumer Response Center toll-free at 1-877-IDTHEFT.

### **4. Recheck your credit report in a few months to:**

- Verify your corrections and changes.
- Make sure no new fraudulent activity has occurred.
- Request a "fraud alert" for your file and a victim's statement asking creditors to call you before opening new accounts or changing your existing ones. This can help prevent an identity thief from opening additional accounts in your name.

### **5. Check your mailbox for stolen mail to:**

- Make sure no one has requested an unauthorized address change, title change, or PIN change or ordered new cards or checks to be sent to another address.
- If a thief has stolen your mail, contact your local post office and police.

### **6. Maintain a written chronology of what happened by noting:**

- What was lost.
- The steps you took to report the incident to the various agencies, banks and firms impacted.
- The date, time, contact telephone numbers, name of the person you talked to and any relevant report or reference number and instructions.

### **7. Send a registered letter to all creditors where fraudulent accounts have been opened and:**

- Include a copy of the police report.
- Include the ID Theft Affidavit.
- Request that the institution send you a letter of release to clean up the account and acknowledge that it is fraudulent.

**IMPORTANT CONTACT INFORMATION****For credit checks and theft information, contact:**

<b>Institution</b>	<b>Email</b>	<b>Phone</b>
Federal Trade Commission	<a href="http://www.consumer.gov/idtheft">www.consumer.gov/idtheft</a>	1-877-IDTHEFT
Equifax	<a href="http://www.equifax.com">www.equifax.com</a>	1-800-525-6285
Experian	<a href="http://www.experian.com">www.experian.com</a>	1-888-397-3742
Trans Union	<a href="http://www.transunion.com">www.transunion.com</a>	1-800-680-7289
Telecheck	<a href="http://www.telecheck.com">www.telecheck.com</a>	1-800-710-9898
International Check Services	N/A	1-800-366-5010
Identity Theft Resource Center	<a href="http://www.idtheftcenter.org">www.idtheftcenter.org</a>	1-858-693-7935
Social Security SSN Fraud Hotline Administration	<a href="http://www.ssa.gov">www.ssa.gov</a>	1-800-269-0271
The National Fraud Information Center	<a href="http://www.fraud.org">www.fraud.org</a>	1-800-876-7060
U.S.Postal SSN Fraud Hotline Inspection Service	<a href="http://www.usps.gov/postalinspectors">www.usps.gov/postalinspectors</a>	1-800-372-8347