Jamaica Bankers
ASSOCIATION

SERVICE.SECURITY.VISION

FRAUD FAQs

The Jamaica Bankers' Association (JBA) and its members have compiled these frequently asked questions to inform our customers about fraud.

Note: These FAQs give information of a general nature and are not intended to be relied on by readers as advice in any particular matter. Readers should contact their own advisors on how this information may apply to their circumstances.

FRAUD FAQS

How can I protect myself?

The most important thing you can do is keep your personal information safe and never share your online passwords and PINs with anyone, not even bank employees as a bank will never ask you for this information. In addition, ensure that you destroy all bank statements, ATM and sales receipts and expired cards before throwing them away. Here are some other tips:

USING A DEBIT CARD AT THE ATM:

- Take a look around as you approach the ATM and if there's anything suspicious, don't use the machine at that time (report any suspicious activity to the police).
- Keep your card in a safe place and never lend it to anyone.
- Protect your PIN — don't write it down or tell anyone what it is.
- Choose a PIN that is not easy for someone to guess (like 1234, your telephone number or your birthday).
- Use your hand or your body as a shield when entering your PIN in case anyone is watching you.
- Keep your receipts and track your transactions online or on your statements so that you can identify suspicious transactions.
- If you lose your card or it is stolen, report the matter to your bank immediately.

USING A DEBIT OR CREDIT CARD AT A RETAIL OUTLET:

- Only use your card at reputable retail outlets where and when you feel secure.
- Keep an eye on your card when it is being swiped for payment. If possible, do not send your card to be swiped (for example, at restaurants). Take it to the cashier's counter or ask the employee to bring the machine to you.
- Keep your receipts and track your transactions online or on your statements so that you can identify suspicious transactions.
- If you lose your card or it is stolen, report the matter to your bank immediately.

ONLINE:

- Use antivirus software and firewalls to protect your computer.
- Be wary of any e-mail from someone you do not know or trust —delete without opening any e-mails that you think are suspicious.
- Never provide personal details including account numbers or passwords, in response to any e-mail.
- Never click on a link or attachment in an e-mail which says it will send you to a bank's website. Only access your bank's website logon page by typing the address into your browser.
- Always memorise your passwords and do not write them down or store them on your computer. Also, change your password regularly and don't use the same password for all sites.
- When shopping online, only use secure websites. Secure websites use protective encryption technology to transfer information from your computer to the online merchant's computer system, which keeps safe confidential information such as credit card details. Identify a secured website by looking for "https" in the web address or URL (an unsecured website address starts with "http").

FRAUD FAQS

What should I be looking for?

Signs of fraudulent activity include: withdrawals on your bank account or charges to your credit card that you did not make and notices about new accounts or credit cards that you did not apply for. Another common sign is when your card "declines" and you cannot make a payment even though you are sure you have funds available. If you observe any of these signs, you should report the matter to your bank immediately in branch or by phone (most banks have a 24-hour customer service line).

What are the banks doing to help protect me from fraud?

Over the years, we have taken many steps to protect our customers and we continue to implement new strategies for your protection. These measures include: staff training and customer education; strict privacy policies; rigorous security and encryption systems; constant upgrading of ATM, credit card and online account security; video surveillance at branches and ATMs; monitoring of account activities to identify suspicious or unusual transactions; dedicated resources for investigation of fraud cases; and prosecution of criminals.

Where can I get more information on fraud and identity theft?

DETAILED INFORMATION ON FRAUD AND IDENTITY THEFT CAN BE FOUND AT
HTTP://WWW.JBA.ORG.JM/

FRAUD FAQS

Can I become a victim of fraud?

Yes. Every year millions of consumers around the world become victims of fraud through identity theft.

Identity theft happens when criminals get your personal information without your permission and pretend to be you. They will most likely use this information to commit crimes which can have negative effects on your finances, your credit rating and your reputation. Such crimes include emptying your bank account, charging large expenses to your credit card, using your name and information to open new accounts or make purchases that you will be responsible for, and even using your information to steal, bribe or commit other offences that could put you in trouble with the police.

What kind of information do these criminals want?

In order to take on your identity, these criminals want your name, address, date of birth, identifying number (such as TRN, NIS, etc), your bank account or credit/debit card numbers, your mother's maiden name, your online usernames and passwords, your ATM PIN, and copies of other identification documents such as passports, national identification cards, employee cards, etc.

How do these criminals get my information?

There are numerous methods that are used but some of the most popular are: watching you at the ATM or when you use your debit card to try to get your PIN; making copies of your debit and credit cards when you make purchases; sending you e-mails with links to fake websites to log in; and stealing your information when you use computers that are unprotected or buy from websites that are not secure.