

Security Message: Credit Card/ATM Fraud in The Bahamas

July 14, 2014

The U.S. Embassy is aware of several recent instances of credit card fraud in Nassau. U.S. citizens have reported that they have received fraudulent credit card charges on their credit cards and that their respective credit card companies notified them of attempted fraud related charges on their accounts after using their card at various businesses in Nassau.

The Embassy urges all U.S. citizens to check their credit and debit card accounts for any unusual activity. If you suspect fraudulent activity, contact your bank immediately to close the compromised credit card account and place a fraud investigation with your credit card company.

The Royal Bahamas Police Force recently issued a similar warning regarding an increase in credit and debit card fraud matters reported to the police.

Please consider the following tips to safeguard your credit and ATM Cards:

- Cancel accounts you do not use or need. Carry only the cards and identification you need when you go out.
- Do not let your card out of sight. A person taking it to a Point of Sale (POS) device might have a skimmer to steal the information on the magnetic strip, copy your card number and the 3-digit security number on the back of the card, or switch cards. If you do give your card to a waiter or other sales person, make sure you get your card back.
- Never loan your card to anyone.
- Pay attention to billing cycles. Check with the credit card company if you miss a bill to make sure that your address has not been changed without your knowledge.
- Only put the last four digits of your account number on checks you write to your credit card company. It knows the whole number and anyone who handles your check as it is processed won't have access to the number.
- Notify your credit card companies and financial institutions in advance of any address or phone number changes.

- Bring home all credit card receipts and match them against your monthly statements. Look for charges you did not make. Dispose of them at home. Never toss your receipts in a public trash container.
- Call the credit card company or bank involved if a new card you applied for hasn't arrived in a timely manner.
- Monitor the expiration dates of your cards and contact the card issuer if new cards are not received before your card expires.
- Report all lost or stolen cards immediately and request cards with new account numbers. In this case the federal Truth in Lending Act limits your liability to \$50 of any charges made before you report your card lost or stolen. Contact the issuer if replacement cards are not received in a reasonable time.
- Sign and activate new cards promptly on receipt. Or write "See ID" on the signature line on the back of the card. Then a thief won't have your signature. A merchant will ask you for a picture ID to make sure you are the cardholder.
- Never put your card number on a post card or on the outside of a mailing envelope.
- Tear into small pieces or shred any pre-approved credit card offers. They can be used by thieves to order cards in your name.
- Ask your credit card company to stop sending blank checks.
- Have your name removed from lists supplied by the Consumer Credit Reporting Companies (Equifax, Experian, Innovis, and TransUnion) to be used for pre-approved/pre-screened offers of credit or insurance. Call **(888) 567-8688** or go to www.optoutprescreen.com to do this.
- Make sure your bank and credit card companies have your latest home and cell phone numbers, and e-mail address so they can contact you quickly if they suspect fraud in your accounts.
- Some credit cards now have embedded Radio Frequency Identification (RFID) chips that are designed to be read by secure card readers at distances of less than 4 inches when properly oriented for "contactless payments." Thus, RFID readers that are available to the general public and can operate at ranges up to 25 feet and are essentially useless in stealing the information on your card. Even if that information is "hi-jacked," the cards are said to have security features that make it difficult or impossible to make a

fraudulent transaction. Furthermore, the information on the chip is not the same as that on the magnetic strip, and it cannot be used to create a functioning counterfeit version of the card. If you have a card with a RFID chip and do not want to risk having the information on it stolen and used in any fraudulent activity, ask your card company for a new card without a chip.

Using an ATM

- Use ATMs that are inside a store or a bank. These are less likely to have been tampered with for skimming, which is the illegal capture and utilization of a cardholder's financial information from an ATM transaction. If you use an outside ATM, it should be well-lighted and under video surveillance.
- Check the machine and everything around it before you take out your card. Look for parts that seem crooked or have a different color, or decals that are partially covered. If something does not seem right, go to another machine.
- Most ATMs have flashing lights in the card slot. Their obscuration is a sign of tampering.
- Look to see if there is anything in the slot where you insert your ATM card. Thieves place a small, hard-to-detect skimming device in the card slot to steal your PIN and other bank account information. If anything looks suspicious, give it a pull or push. Skimmers are usually held in place loosely by glue or tape to make them easy for the thief to remove. If you remove one, contact the SDPD immediately. Do not throw it away or keep it; that would make it look like you are running the scheme.
- Check for a false keypad that has been installed over the built-in one. False keypads stick out too far or look strange.
- Check the area around the machine for hidden cameras. To be safe shield your hand when entering your PIN so it can't be seen by anyone near you or by a hidden camera.
- Memorize your PIN and keep it secret. Do not write it down or keep it in your wallet or purse.
- Keep the customer-service phone numbers of your bank and credit-card company readily available. Call the appropriate number immediately if your card gets stuck in an ATM. Do not leave the ATM.

- Monitor your bank statements frequently and report any unauthorized activity immediately.

If you become a victim of identity theft

- Set up a folder where you can keep a log of all your contacts and documents.
- Contact the Federal Trade Commission (FTC) to report the theft. Its Identity Theft Hotline is **(877) 438-4338**. Or visit its website at www.ftc.gov/idtheft. The FTC is the federal clearinghouse of complaints of victims of identity theft. It helps victims by providing information to resolve financial and other problems that could result from identity theft. Its booklet entitled *Take Charge: Fighting Back Against Identity Theft* deals with bank accounts and fraudulent withdrawals, bankruptcy fraud, investment fraud, phone fraud, and other specific problems. It also describes the immediate steps victims should take and ways to minimize recurrences.
- Report the theft to the fraud units of Equifax at **(800) 525-6285**, Experian at **(888) 397-3742**, and TransUnion at **(800) 680-7289**. Ask to have a fraud alert placed on your credit reports. It will tell creditors to follow certain procedures before they open new accounts in your name or make changes to you existing accounts. In placing a fraud alert you will be entitled to free copies of your credit reports. Review them carefully. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain. Fraud alerts are good for 90 days and can be renewed. This is a free asset.
- Alert your banks of any fraud and request new account numbers with new checks, ATM cards, and PINs. Also provide new passwords and stop payment on any missing checks.
- Contact all your creditors by phone and in writing to inform them of the theft.
- Call your credit card companies and request account number changes. Do not ask to cancel or close your accounts; that can hurt your credit score, especially if you have outstanding balances. Say you want a new numbers issued so your old numbers will not show up as being "cancelled by consumer" on your credit reports.

- Call the security or fraud departments of each company you have a charge account with to close any accounts that have been tampered with or established fraudulently. Follow up the request in writing and ask for written verification that the accounts have been closed and any fraudulent debts discharged. Keep copies of all documents and records of all conversations about the theft. If you still want a charge account, request a new number.
- Report the loss of your SSN to the IRS. This will alert the IRS that someone might use your SSN to get a job or file a tax return to receive a refund. Call its Identity Theft Hotline at **(800) 908-4490** and go to <http://www.irs.gov/privacy/article/0,,id=186436,00.html>. Follow the directions there regarding identity theft and your tax records, and the need to provide it with proof of your identity. Also contact the Social Security Administration (SSA) on its Fraud Hotline at **(800) 269-0271** or by e-mail to the Office of the Inspector General at www.ssa.gov/org.
- Call the SSA at **(800) 325-0778** if your Medicare card is lost or stolen. Ask for a replacement.
- In the case of medical identity theft request a copy of your current medical files from each health care provider, and request that all false information be removed from your medical and insurance files. Enclose a copy of the police report with your requests. For more information things to do if you are a victim of medical identity theft or concerned about it go the World Privacy Forum's website at www.worldprivacyforum.org/medicalidentitytheft.html
- Call the Health Insurance Counseling and Advocacy Program's Senior Medicare Patrol (HICAP/SMP) at **(800) 434-0222** to report any fraud involving Medicare.

Additional tips on avoiding and resolving identity theft problems are available on the Identity Theft Resource Center (ITRC) at www.idtheftcenter.org. It contains information ranging from advice for people who have had a wallet stolen to tips for reducing the risks of identity theft. It also contains fact sheets, solutions to various identity theft problems, letter forms, scam alerts, a "Help, I'm a Victim of Identity Theft" button, and answers to frequently asked questions. Its toll-free victim-assistance number is **(888) 400-5530**.

If you are the victim of any crime abroad (including the loss or theft of a U.S. passport), you should immediately contact the local police (dial “911”). Contact with the Embassy should be made as soon as possible thereafter.

We strongly recommend that U.S. citizens traveling to or residing in The Bahamas enroll in the [Department of State’s Smart Traveler Enrollment Program \(STEP\)](#). STEP enrollment gives you the latest security updates, and makes it easier for the U.S. embassy or nearest U.S. consulate to contact you in an emergency. If you don’t have Internet access, enroll directly with the nearest U.S. embassy or consulate.

Regularly monitor the State Department’s [website](#), where you can find current Travel Warnings, Travel Alerts, and the Worldwide Caution. Read the [Country Specific Information for The Bahamas](#). For additional information, refer to [“A Safe Trip Abroad”](#) on the State Department’s website.

Contact the U.S. embassy or consulate for up-to-date information on travel restrictions. You can also call 1-888-407-4747 toll-free in the United States and Canada or 1-202-501-4444 from other countries. These numbers are available from 8:00 a.m. to 8:00 p.m. Eastern Time, Monday through Friday (except U.S. federal holidays). Follow us on [Twitter](#) and [Facebook](#), and download our free Smart Traveler App, available through [iTunes](#) and [Google play](#), to have travel information at your fingertips.

In The Bahamas, the Embassy is located at 42 Queen Street in downtown Nassau, and can be reached at 242-322-1181.