



Embassy of the United States of America

American Citizen Services
24 Grosvenor Square
London, W1A 2LQ

CREDIT/DEBIT CARD FRAUD IN THE UNITED KINGDOM

CREDIT/DEBIT CARD FRAUD

Credit/debit card fraud is a growing problem that can affect American citizens living both in the United States and abroad. In fact, the U.S. Embassy in London frequently receives reports of U.S. citizens in the United Kingdom who have been victims of debit card fraud originating in the United States.

For example, one U.S. citizen checked her bank account online to find three, \$500 charges at a large box store in Wisconsin from the week before. The victim had not been back to the United States during the previous year, and never to Wisconsin, yet the store reported that a woman identifying herself as the victim appeared in person with the debit card to make the purchases.

As is the case with many U.S.-issued credit/debit cards, the victim's card in the above scam did not have a PIN associated with it. Many U.S.-issued credit/debit cards also lack a microchip, common among UK-issued cards, as an additional security feature.

While we are aware of no fraudulent transactions originating in the United Kingdom, we recommend that all Americans take the following precautions:

- Only use your credit/debit card for purchases at reputable establishments, including Internet-based retailers.
- Frequently check the balances and purchases on your credit/debit cards to identify potential instances of fraud in a timely manner.
- Ensure that your bank or financial institution no longer sends statements or other documents containing personal information to former addresses.
- Verify the amounts of your personal liability with your financial institutions in cases of fraudulent transactions.
- Report instances of credit/debit card fraud immediately to your bank or financial institution.
- Do not give your PIN to anyone over the phone. Often thieves steal the cards and then call the victim for their PIN, sometimes claiming to be law enforcement or the issuing bank.

- Memorize your PIN. Do not use your birth date, address, phone number, or Social Security number. Never store your PIN with your card, and do not make it available to others.

CASH MACHINE FRAUD

ATMs have become one of the most convenient and efficient ways for travelers in the United Kingdom to obtain local currency. Most cash machines accept American bank cards and will give you pounds while deducting dollars from your U.S. account. However, use of these machines is not without risk. ATM fraud in the United Kingdom has increased significantly over the past few years and is becoming more sophisticated, incorporating technologies to record surreptitiously customer ATM card and PIN information.



A normal ATM device.



ATM with skimming device attached in front of card slot. Notice how the card slot is no longer inset into the machine, but “bulges” outward.

ATM fraud in the United Kingdom generally comes in three varieties: card-reading devices, card-trapping devices, and distraction schemes.

1. **Card Reading Devices**: Criminals alter the cash machine itself by adding a skimming device and a mini-camera to it. The first device, mounted on the card entry slot, reads the bar code on your card. The second records your PIN. After you complete your transaction, receive your card, and walk away, someone else has your number and your access code. Usually, the perpetrators make a new card and use it to withdraw money from your account. The skimming devices are not always easy to spot, especially if you are unfamiliar with the look of UK cash machines.
2. **Card-Trapping Devices**: An alternative form of altering the cash machine itself involves inserting a thin ribbon of x-ray tape into the card slot. The loop traps your card and makes it seem as though the bank has repossessed it. At this point, someone else, a purported “Good Samaritan,” comes along and tells you that you can retrieve your card by re-entering your PIN code. He watches while you do so.

After your card still refuses to emerge and you walk away from the ATM, the perpetrator removes the device and your card, which he then uses to withdraw money from your account.

3. Distraction Schemes: Distraction schemes do not rely on tampering with cash machines themselves; instead, they you are interrupted while withdrawing funds. Typically, there are two perpetrators, one who distracts you after you have entered your card and PIN, and another who grabs your money. The distractor may pretend to sell or give you a newspaper; place a £5 note at your feet and tell you that you dropped some money; ask you for a charitable donation; or whisper in your ear. Sometimes the distractors are children. The common element in all these ruses is that they occur after you have entered your card and your PIN.

In order to prevent becoming the victim of such scams:

- If possible, use ATMs located inside buildings or in bustling public places where it is difficult for criminals to tamper with the machines. Do not use machines in isolated areas or at night.
- Avoid cash machines where the card slots appear to have been mounted on the machine (see illustration above). Card entry slots should be flush with the surface of the ATM or recessed from it. If you see a card entry slot that is raised above the machine, do not use it.
- If you find it difficult to read the screen or enter your PIN, do not use the machine. It may have been altered. Legitimate displays are never mounted in front of ATMs. Anything that blocks or partially obscures a sign may house a camera.
- Guard your PIN, especially when entering it, by shielding the keypad with one hand.
- If possible, have someone accompany you while you make a withdrawal.
- If you are distracted at all during a transaction, immediately press cancel and collect your card before responding to anyone who has accosted you.
- If a machine swallows your card, call the bank's toll-free number (usually posted on or near the cash machine) and report it.
- Change your PIN from the original number given when you first got your card (this number is sometimes contained in the data on the magnetic strip and can be discovered by thieves who have stolen your card). Do not keep your account number and PIN together.

If you do find yourself the victim of ATM fraud, do the following:

- If you discover a card reader or card-trapping device, do not remove it. The criminals may be watching the location and will want to recover their equipment. Instead, call the police at 999.

- Call your bank to alert it that you have lost your card and to refuse all new withdrawals. This will be easier if you carry the bank's phone number with you on your trip.
- If someone whose behavior raises your suspicion approaches you at a cash machine, do not challenge the person but keep track of the details and report the matter to the police as soon as possible.
- If you discover the fraud after you return to the United States, you can (and should) still file a police report in the United Kingdom. To do so, go to http://www.met.police.uk/reporting_crime/index.htm#online.