



In This Issue, You Will Learn About:

- > FICO Scores for Experian
- > ATM's are key Targets for Skimmers
- > Data Breaches

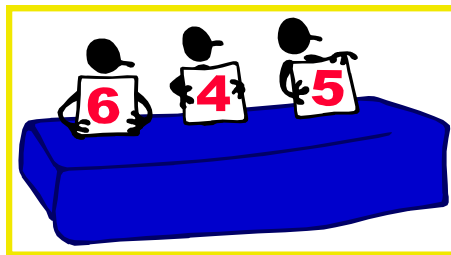
FICO Scores for Experian?

In today's economy good credit is more important and prevalent than ever. The three major credit bureaus that service consumers today are Experian, Equifax, and TransUnion. Since 2005 federal laws have been enacted that require bureaus to offer free credit reports to consumers yearly. The laws were put into place to ensure that consumers had access to their credit files and could defend against both credit errors and identity theft.

Lenders use your credit report and credit scores to access your level of risk. Obviously, the better the borrowing history, the lower the risk you pose to the company. How is your risk assessed you ask? Well in two words, FAIR ISSAC. Fair Issac created what is known as the Fair Issac Corporation Score, or most commonly known as the FICO score. This score is regarded as the most accurate risk assessment score to date. The score is provided to all three major bureaus separately dependent upon the credit recorded on the consumers' behalf. Therefore, each bureau usually dawns a completely different score for the same consumer. Majority of lenders rely on these scores before making a decision if they will lend, and how much they can afford to lend based on the risk involved.

In 2006, the Vantage Score was introduced by the credit bureaus as an internal attempt to create an alike, but arguably better score to measure consumer credit risk. The score attempted to offer a new credit score model that was supposed to be more

accurate and fair to consumers. The new system was supposed to reduce the confusion for borrowers and lenders by creating one common score rather than three different scores. When Fair Isaac found this out, they sued the three major credit bureaus the same year claiming that the Vantage Score harmed the FICO brand and disrupted the consumers' ability to get the most accurate information in regards to their credit. Fair Isaac did however decide to drop Equifax from the suit, but charges are still pending against TransUnion and Experian. Fair Isaac continues to provide scores for TransUnion and Equifax, but have ran into a stalemate with Experian who will no longer share credit information with the company.



As of February 15, 2009, Experian stopped selling its consumer credit data to Fair Isaac. They will however, still sell non accessible data on consumer lending and borrowing to different business that request. Experian still provides free credit reports, and consumers wanting their Experian FICO score were urged to purchase it from FICO before February 14, 2009. As for now, that score is extinct.

Inside this issue:

FICO Scores for Experian?	1
ATM's are key Targets for Skimmers	2
Data Breaches	3

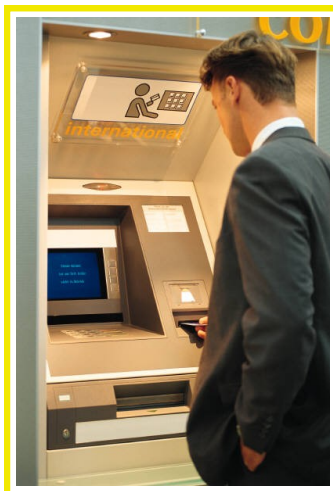
ATM's are key Targets for Skimmers

Banks make sure that we have 24 hour access to our money through Automatic Teller Machines (ATM). Unfortunately, identity thieves may also have 24 hour access to your funds by using skimmers if you aren't careful, and paying attention to detail. In this article we will be educating you on how to be aware and cautious when using ATM's because they have become another prime target for identity thieves.

Most people would find it very difficult to identify skimming devices because they are hard to recognize and come in different forms. They are made to blend in and go unnoticed on their respective host machine. Skimming devices are maliciously placed on the card reader of ATM's to secretly gain access to your account information when you use an ATM. These devices illegally capture information from your debit and/or credit cards and store it for the thieves' retrieval. Skimming devices will do this by using the magnetic strip on the back of the card to electronically store information that is transmitted to the device. These magnetic strips contain three smaller strips that convey the necessary information needed to process each transaction made with a merchant. This is where all the account holder information is held: name, account number, expiration, and PIN. When your PIN is punched into the keypad, skimming devices are designed to record that information as well. With your account number, expiration, and PIN a thief has all they need to replicate your card and drain your account. It's as easy as using the skimming device to capture and store your information as it is for you to click save on your home PC and save a file. These devices are hard to notice if you do not know what you are looking for because criminals

have done a great job of mimicking the looks and likeness of an authentic machine.

Altered ATM's are another place where skimmer devices are placed strategically in order to be hidden from potential users. These ATM's may appear to be legitimate; but, will usually be missing key parts that may help you identify them. For instance, though most would consider this a trivial step, to make sure there are money retrieval slots and receipt receptacles. These are tale-tale signs of altered ATM's. Also take the time to familiarize yourself with some of the known ATM companies that has issued authentic units. Although bank's names like Bank of America, Wachovia, and SunTrust are easy to spot because we see them all the time, other ATM's owners are third party. The third party ATM's owners purchase ATM's brands like Nautilus, NCR, Triton, Tidel, Tranax, or WRG. These are some brand labels you may see on the ATM's that you should familiarize yourself with. Though identity thieves have gotten smart enough to place fraudulent ATM's that have an authentic look and even name, some do not and this is definitely an indicator that should raise red flags.



When going to an ATM here are some tips:

1. Make sure you keep your PIN safe by being very cautious while inputting it into the machine.
2. Be cautious if help is offered because this can be a sign of a thief trying to steal your information.
3. Do not let your credit or debit card out of your sight when processing in any ATM's.
4. Make sure that the card is returned after the transaction is completed and if not immediately contact the ATM company by locating the telephone number on the ATM's.
5. Make sure that credit and/or bank statements are being checked regularly.
6. Be cautious of using the machine if unusual signage is on the ATM's.
7. Take a hard look at the ATM to ensure that everything looks authentic.
8. If you do not feel comfortable with an ATM, do not use it.
9. Report any ATM's that you think looks suspicious.
10. Try to use ATM's that you are familiar with or use regularly.

By following these helpful tips, you will reduce the chances of losing your information to an identity thief. If you do become a victim, make sure and call your friends here at National ID Recovery. Our Recovery Specialists are waiting for your call and ready to restore your identity to a pre-theft state.

Published Data Security Breaches Reported for 2008

There have been approximately 300 Published Data Breaches since January potentially exposing more than 12.5 million individuals to identity theft.

Date	Company	Type of Breach	Citizens Exposed
2/06/09	Kaiser Permanente	Stolen File	30,000
2/09/09	Parkland Memorial Hospital	Stolen Laptop	9,300
2/09/09	Federal Aviation Administration	Hack	43,000
2/10/09	Royal Bolton Hospital	Disposal Document	1,300
2/11/09	City of Regina, Saskatchewan	Unknown	1,000
2/14/09	University of Alabama	Hack	37,000
2/16/09	Wyndham Hotels & Resorts	Hack	21,000
2/17/09	Broome Community College	Snail Mail	14,000
2/18/09	Northeast Orthopedics, LLP	Web	1,000
2/18/09	Rio Grande Food Project	Stolen Laptop	36,000
2/19/09	University of Florida	Hack	97,200
2/20/09	Arkansas Department of Information Systems	Lost Tape	807,000
2/23/09	Ryerson University	Web	588
2/25/09	Steamboat Springs School District	Stolen Laptop	1,300