Protecting Our Customers

When a check is cashed in the bank, our tellers have immediate access to the signature card for verification. We have exception reports that show us any unusual activity on an account. We also make sure that any company we do business with or that we may have to share customer information with in order to process transactions has procedures in place to protect the data we give them.

For More Information

Fraud can often lead to identity theft which is a growing problem in this country. We have a section on our homepage dedicated to identity theft which includes a video as well as an information packet you can print that will walk you through the steps of what to do if you are a victim of the ever-growing crime.

Strength & Stability since 1927

To learn more
visit our website:

www.bankofutica.com

Bank of Utica

222 Genesee Street
Utica, New York 13502
Phone: 315-797-2700

Open: Mon-Fri 9:00—5:00
Drive-through 5:30 on Fri

Protecting You From Fraud

BANK OF UTICA
Bank of Utica
MEMBER FDIC

In a league all our own®

Protecting You From Fraud

Bank of Utica is strongly committed to doing everything we can to protect our customers, to guard against fraud, and to make banking with us secure and safe. This brochure outlines some of the many methods we use to protect you. Of course, we would not want to make public all the security measures used, as we believe many of them should best be kept secret.

We use many tools in our fight against fraud, from state-of-the-art technology to good old fashioned common sense. We keep up on the latest software, firewalls, and security systems while also relying on the knowledge and expertise of our staff who are familiar with many types of fraud and can often spot unusual account activity. We also monitor large software companies such as Microsoft and Adobe for patches to their systems designed to strengthen any weaknesses which may attract viruses or hackers.

Our sophisticated firewalls and antivirus software can detect possible intrusions 24 hours a day and can immediately shut down our website if necessary. We also hire experts to try to hack into our system and find weaknesses. The methods they use are designed to stay one step ahead of the most sophisticated computer hackers.

Technology

- We use software that monitors for fraudulent checks. This software tries to determine if a signature is genuine or even if the check stock (paper) is the same as the checks you have used in the past. Another type of software we use can detect unusual patterns of debit card activity—whether it's for one customer or a large scale fraudulent scheme against many banks, we can quickly take action to close debit card accounts and reissue cards.
- We use a multi-layer security system designed to identify you in a number of ways including your login credentials, what type of device you are using and if you are logging in from a familiar location.
- For our online banking customers, we offer IBM software, called Trusteer Rapport. Trusteer adds an important layer of security that is capable of detecting, alerting, and preventing even the most sophisticated financial attacks. From the moment it is installed, it protects your computer and mitigates financial malware infections without interfering with any existing anti-virus software. You can be assured that any transaction you conduct from our website—whether inquiries, transfers, or bill payments—will be protected and secure.

Our Employees

We feel that our employees are extremely effective when it comes to protecting our customers. Half of our employees have been with us over twenty years and 75% over ten years. They understand banking and personally know many of our customers and their banking patterns. If unusual activity is suspected, they are trained to look further and determine if there is a problem.

Employees are also trained on how to identify our customers, how to spot possible cases of identity theft, and how to deal with fraud. We stress the importance of never leaving customer information unattended, whether on a desk or on a computer screen. All hard copies of customer information are securely stored or destroyed.

Some of the procedures we use to detect fraud include looking at large checks every day to be sure that the signatures are authorized, that they are properly signed and endorsed and have not been altered. We carefully monitor address changes and never send personal information via email. To further protect yourself, we encourage you to use passwords, which we will verify before giving out account information.