Product

Multifactor Authentication

Flexible Options for Effective Online Fraud Mitigation

Fiserv offers several advanced alternatives to help you protect against online banking fraud. With Multifactor Authentication from Fiserv, you can enhance online security and maintain compliance with banking regulations without devoting significant resources to the process.

A dramatic rise in costly and constantly evolving forms of online banking fraud challenges bankers to strengthen their defenses and maintain a high level of customer confidence – all while keeping costs down. Multifactor authentication (MFA), which provides an additional level of customer authentication in addition to the standard user name and password, is one of the most effective ways to prevent fraudulent online activity.

Multifactor Authentication delivers several cost-effective options designed to protect you and your customers who use Retail Online™ and Business Online™ from Fiserv. Our portable security tokens generate one-time passwords that customers must enter to log in to their account or complete high-risk transactions. Another method employs PC forensics to seamlessly authenticate the customer's computer or other device being used to access online accounts.

Ultraportable Security Tokens Offer Customer Convenience

With MFA Security Tokens from Fiserv, a small, lightweight device generates a series of random numbers that serve as a one-time password (OTP). A step up from the traditional and seldom-changing static password, the OTP changes each time a customer logs in. Available through our partnership with VASCO Data Security International, MFA Security Tokens can be used with your Business Online banking customers. This secure MFA method requires corporate customers to enter the OTP in addition to their standard user name and password at login. You can also require OTP entry for customers when making designated high-risk transactions.

User-Friendly Cordless Device

MFA Security Tokens are powered by battery, providing a cordless "air gap" between the token and the network.

This eliminates the possibility of connecting to a hosting device that might be infected. Tokens are also portable and cannot be duplicated, remotely hacked or spoofed. They are available for licensing in a variety of styles, with customization options to fit your unique branding.

Deploys in Seconds

Tokens are activated by customers through their Internet banking account. It takes just a few seconds to provide the token's serial number and define a personal identification number (PIN). A security question and email address are also collected to assist in reporting a lost or damaged token.

DIGIPASS GO 3

Customer adoption of security tools is crucial to guaranteeing deployment success, and the DIGIPASS GO 3 is a popular option with customers. The device is affordable, easy to use, and both quick and efficient to deploy. It can also be customized with corporate logos, branding and colors to suit your needs.

DIGIPASS 260

Another cost-effective alternative, the DIGIPASS 260, is a password-protected token that features PIN pad technology. Customers logging in to their online banking account enter their user name and password, and an OTP generated by the token.

To authenticate customers making high-risk transactions, you can choose from several levels of MFA security, including OTP, challenge-response OTP and digital signature OTP. The challenge-response and digital signature methods employ stronger OTPs, which are generated by the security token after a customer successfully enters requested information.

Key Benefits

- OTP generation
- Mutual customer and website authentication
- MFA at login and for high-risk transactions
- Small, lightweight device with extended battery lifetime
- Activated by pushing one small button
- 3-DES encryption
- Time-synchronous authentication
- Challenge-response and digital signature OTP options
- Physical PIN entry available
- Customer self-service password change
- Multiple invalid password attempts trigger lockout
- Dual-function on-off and erase button

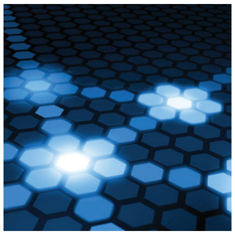
PC Forensics Provides a Seamless Customer Experience

MFA Device Security from Fiserv, an option that's perfect for high-volume deployment, is available for your Retail Online and Business Online banking customers through our partnership with RSA Security. To verify a customer's identity, this proven solution uses a traditional user name and password, and also compares an electronic fingerprint of the customer's PC to the device being used to log in. The result provides end-to- end protection against phishing, spoofing, keyboard logging and other fraudulent attacks, without the need to install any new software.

Electronic Device Fingerprint Streamlines Authentication

MFA Device Security quickly registers the customer's computer using secure cookies and Adobe® Macromedia® Flash™ shared objects. In addition, a number of inherent device characteristics are assessed to create a one-of-a-kind electronic fingerprint that validates the device authenticity each time a customer logs in. This prevents criminals from logging in to a customer's account, even if they know the user name and password.

For customers who have multiple computers, supplemental authentication quickly confirms their identity when using a device that is not yet registered by MFA Device Security. They must correctly answer a challenge question defined during enrollment in order to log in from a new computer. Once the new device is registered, authentication during future logins takes less than a second for the vast majority of customers.



Fiserv is driving innovation in Payments, Processing Services, Risk & Compliance, Customer & Channel Management and Insights & Optimization, and leading the transformation of financial services technology to help our clients change the way financial services are delivered. Visit www.fiserv.com for a look at what's next now.

Fraud Monitoring and Anomaly Detection Identifies Suspicious Activity

Fraud monitoring assists your institution in identifying and investigating patterns of suspicious activity. Monitor and analyze a wide range of customer activities, from logins, password changes, email address changes to transactional activities such as transfers, approvals, stop payments and more. You also have the ability to monitor raw ACH files for possible fraud before the file is released to the Fed.

Malware detection and removal provides your customers with endpoint security and protection against threats and viruses normal anti-virus tools fail to detect. The user's device is scanned to check for any viruses and malware and removes them completely before allowing your customers to perform any online banking activity.

Connect With Us

For more information about Multifactor Authentication, call 800-872-7882, email getsolutions@fiserv.com or visit www.fiserv.com.

fiserv.

Fiserv, Inc.
255 Fiserv Drive
Brookfield, WI 53045

800-872-7882
262-879-5322
getsolutions@fiserv.com
www.fiserv.com