Evolving security threats require the use of evolving controls and methods to protect all transaction activity issued by retail and business online banking customers.
The Internet has become the preferred, essential channel for banking transactions, but that evolution has brought about a dramatic increase in the number of attempts to gain access to critical banking data and in the sophistication of those threats. These online banking security guidelines and best practices are furnished as part of Fiserv’s ongoing commitment to provide you with tools, information and services that will help your financial institution operate as securely and efficiently as possible.

Based on our review and analysis of the changing environment, we endeavor to provide solutions that protect against and minimize fraudulent access to that information, and to provide guidance that improves our clients’ ability to secure systems, customer data and deposits. This document offers certain recommendations based on online security best practices for consumers and businesses, as well as guidance specific to Retail Online and Business Online, two of Fiserv’s most popular and widely used Internet banking solutions.
Security Guidelines and Best Practices for Retail Online and Business Online

An Online Banking Security Overview

Evolving security threats, both internal and external, require the use of new controls and the latest methods to protect all transaction activity issued by retail and business online banking customers. Multifaceted and layered security tools and procedures strengthen a financial institution’s defenses against these threats by providing multiple checkpoints at different levels to ensure transactions are authorized by a valid user.

Verify that your security practices are stringent by utilizing a strong, multi-layered security strategy, including the use of tokens, one-time passwords, or out-of-band systems to gain access and initiate external fund transfers. A strong security strategy requires that all high-risk transactions be reviewed and authorized by the customer, and that the financial institution use industry-standard practices to validate the legitimacy of those transactions. A layered security policy should also take into consideration where your data is stored, administrative staff, and the physical assets of the organization, including laptops, tablets, mobile phones, WiFi and access to all facilities.

Securing technology systems and protecting the data and assets of customers remains one of the highest priorities for any financial institution. As your technology partner, Fiserv offers advanced security to help you protect your systems and customers, along with useful guidance resulting from the depth and breadth of our experience with the financial services industry and the technologies that drive it. Please contact your Fiserv account manager or support team for additional guidance regarding products and procedures.

As a Fiserv client using Retail Online and Business Online to serve your customers, this best practices guide offers a set of recommendations intended to help you successfully navigate the complexities of financial and information security, and provide the most comprehensive protection possible. This is not intended to be a direct response to any laws or regulatory guidance. It is an overview of our review of the current security environment and select solutions available from Fiserv. To be successful, security measures and compliance must always be evaluated, determined and managed by your financial institution.

Recommendations for the Retail Online and Business Online Internet Banking Solutions

• Regularly review and update your organization’s security risk assessment, including policies and procedures, to be as prepared as possible to confront new online threats.

• Know your customers. Review their previous transactions by inquiring into their transaction history or historical transaction reports. Carefully grant access to money movement solutions, selecting only those customers you know and have a history with.

• Employ multiple and layered security tools.

• Keep operating systems up to date on all recommended patches. Urge your customers to follow this same practice to protect their computers.

• Utilize firewall and intrusion detection services as an additional security layer for blocking and identifying potential online attacks.

• Install and use up-to-date antivirus software (including anti-spam and anti-spyware programs) to prevent, detect and remove malware of all kinds. Urge your customers to follow this same practice to protect their computers.
• Educate your employees and customers about online security measures. Track successful employee participation and reward customers for protecting their own systems.

• Utilize an effective Multifactor Authentication (MFA) process. For customers using MFA Device Security, we strongly recommend use of the emailed one-time password (OTP) as the challenge method, rather than the question-and-answer (challenge-response) method.

• Use of a transaction monitoring product provides anomaly detection, for both the log in and at the transaction level. The MFA Device Security 2.0 release (Q1 2013) upgrades clients to the latest RSA version and includes separately licensed transaction monitoring features.

• Use a centralized fraud detection network such as FraudNet™ from Fiserv to help protect your bill payment customers from fraud before they are affected.

• Utilize positive pay and ACH filtering products to provide your customers with positive pay, debit blocks and transaction frequency limits on specific accounts.

• Require frequent password changes for both employees and customers.

• Premier® and Precision® clients using Retail Online should enable Business Process Manager workflows that require procedures and additional controls for all address maintenance performed by the customer.

• Utilize the Online Banking Risk Assistant, a browser-based tool offered in partnership with Beaver Creek Marketing (www.bankall.com) that enables you to assess your online products and assign accurate risk ratings for each, as called for by FFIEC recommendations.

• Make use of the consumer- and business-oriented tutorials in our Online Education Center, offered in partnership with Beaver Creek Marketing, to help educate customers about electronic banking security, including prevention of key logger, spyware and phishing activity.

Further Recommendations Specific to Commercial Banking and Business Online

• Validate business practices associated with wire transfers, including dual approvals for all wire and ACH transfers, ensuring that dual approvers access and approve from different machines.

• Regularly verify the access permissions and review thresholds defined for each business customer.

• Review audit reports of any recent external and internal user or account maintenance.

• Limit Internet access for business customers’ computers to websites approved for business use, and block all other websites.

• Discourage password-sharing among employees.

• Prevent or discourage the use of laptops and iPads® to access sensitive information over unsecured WiFi systems.

• Limit business customer access to established business hours.

• For customers with high-dollar, high-risk ACH and wire transfers, require use of a password-protected MFA token, for example, the VASCO® Digipass Pro 260, or “DP 260.” These tokens enable challenge-response or digital signature transaction verification.

• For all external transfers, require bank-side and/or customer-side approvals.

• Utilize positive pay to import issued checks, view check images and review check exception items.

• Require a secondary approval for any new or modified transfer templates in ACH Manager and Wire Manager.

• Establish approval options for new or updated ACH Manager and Wire Manager users at the institution level in ACH Administrator and Wires Administrator.

• Take advantage of the complimentary Online Business Banking Security Awareness training course, offered in partnership with BVS Performance Systems (www.bvs.com), for the benefit of Fiserv client financial institutions and their business banking customers.
Recommended Financial and Information Security Practices for Online Banking Consumers

You no doubt provide online banking services to a very large part of your retail customer base, and it’s likely that your business customers also use your retail services. When it comes to online security, educated customers are better-protected customers, and that benefits your financial institution as much as it benefits them. The following are best practices that online banking consumers can follow to increase their personal financial and information security. Feel free to reproduce and share these tips as part of your own customer education and support efforts.

Use Personal Financial Information and Financial Services Passwords Only in Secure Transactions

• Personal financial information (such as names in combination with Social Security Numbers, account numbers, and credit or debit card numbers) and passwords for financial services (such as online and mobile banking / payments, and person-to-person payments) should only be used in secure transactions (using the practices described below).

• Personal financial information and passwords for financial services should not be provided in response to unfamiliar or suspicious websites, emails, text messages, telephone calls, mobile phone applications or social media messages.

• If you provide financial information and passwords for financial services in response to unfamiliar or suspicious websites, emails, text messages, telephone calls, mobile phone applications or social media messages, you should change your passwords as quickly as possible.

Use Strong Passwords in All Systems That Require Passwords

• Passwords should use the maximum allowable number and type of characters (such as upper and lower case letters, numbers and symbols) and should not contain predictable terms or numbers.

• A different password should be used for each commercial and financial services website.

• Passwords that are written down or otherwise recorded should not be placed in visible or unsecured locations.

Approach Applications and Links on All Devices and Delivery Channels with Caution

• Approach all applications and links on all devices (such as personal computers, tablets and cell phones) and delivery channels (such as email, text messages and social media sites) with caution, as cybercriminals often use applications and links as the first step in installing malicious software on devices with which fraudulent acts can be enabled.

• Take steps to verify that applications and links posted on social media sites correspond to legitimate websites, and that they have been posted by individuals who are known and trusted.

Use Computers and Online Banking, Bill Payment and Shopping Securely

• Antivirus protection and scanning software that has been reviewed and rated as satisfactory by independent analysts should be installed, updated and utilized as recommended. In addition:

  • If the security software can update automatically, set it to do so.

  • If the security software cannot update automatically, update it after each login.

  • If viruses (also referred to as “malicious software” or “malware”) are detected, the recommendations provided by the antivirus program should be followed promptly.

  • Operating system software updates (also referred to as “patches”) should be accepted, downloaded, installed and run promptly, and as recommended.

  • Personal financial information should never be sent by email in an unencrypted state. An email solution that encrypts messages between financial institutions and their customers should be utilized.
• Financial transactions that are conducted on websites should be conducted on secure websites only. An indicator of a secure website is a URL that begins with “https” in the address, the “s” standing for “secure.” The “https” prefix should be on every page of websites used to conduct transactions, in addition to the sign-in page.

• Privacy policies should be easily found and understood. If the privacy policy is not easily found and understood, then consider conducting business elsewhere. Privacy policies provided by financial institutions in connection with financial services are required to offer consumers a clear method to “opt out” of certain types of information sharing if the institution engages in them.

• Most Wi-Fi networks do not encrypt information and are not secure. Some use encryption and are more secure, WPA being common and WPA2 the strongest. However, if any Wi-Fi network is to be used, a virtual private network (VPN) should be established and used to encrypt communications. VPN encryption applies all the way from the user’s PC to the host computer, regardless of the type of network used. The encryption methods used by VPN are stronger than WEP and WPA.

• Unfamiliar or suspicious emails, text messages, instant messages, phone calls, websites and social media solicitations that request personal financial information should be deleted immediately. They should not be replied to or forwarded, and any links that they contain should not be opened.

• Options to “Remember me” on websites where transactions are conducted should not be used.

• Computer workstations and laptops should be logged off, and preferably not left on, when the user steps away.

• Computer workstations and laptops should be set to logoff automatically after no more than two minutes of non-use, with a password required to log back in.

• Computer workstations, laptops and external storage devices such as USB drives and storage discs should be physically secured with locks (such as with a cable lock or in a locked drawer) when not in use.

• Computers that are no longer in use should have hard drives removed and shredded, or a software program that wipes and eliminates all data from their hard drives should be used, following DOD5220 standards for data sanitization.

Use Mobile Phones, Mobile Banking and Mobile Payments Securely

• Mobile phone applications, text messages, instant messages and calls from unfamiliar or suspicious sources that request personal financial information and passwords should be declined and, when appropriate, promptly deleted, and not replied to or forwarded. Any links they contain should not be opened.

• Each mobile phone and mobile phone application should be assigned a different password with the maximum allowable number and type of characters.

• Mobile phones should be set to logoff automatically after no more than two minutes of non-use, with a password required to log back into the phone.

• Mobile phones should be locked up when not in use and not left in visible, unsecured locations.

• Lost or stolen phones should be reported to the carrier promptly.

Use ATM, Credit, Debit and Prepaid Cards Securely

• Cards should be signed as soon as they arrive.

• Card numbers should only be used in secure transactions and should not be provided in response to unfamiliar or suspicious websites, emails, text messages, telephone calls, mobile phone applications or social media messages.

• If conducted on websites, card transactions should be conducted only on secure websites. An indicator of a secure website is a URL that begins with “https” in the address, the “s” standing for “secure.” The “https” prefix should be on every page of websites used to conduct transactions, in addition to the sign-in page.

• Options to “Remember my card number” on websites where transactions are conducted should not be used.
• Cards should not be left in visible or unsecured locations.

• Lost or stolen cards should be promptly reported to the card issuer.

• Cards that are unused, have been canceled or have been replaced by a new card should be securely eliminated, for example by cutting them into small pieces so they cannot be read.

Use Checks Securely
• Checks should not have Social Security Numbers or driver’s license numbers printed or written on them.

• Checks should not be left visible in unsecured locations.

• Checks that are to be discarded should be eliminated securely, for example by shredding, and should not be discarded in a readable form.

• Checks that are tamper resistant are available at certain financial institutions. These checks include security features such as chemically sensitive paper to deter alterations.

Use Statements and E-Statements, Bills and E-Bills, and Transaction Receipts Securely
• Statements, e-statements, bills and e-bills should be reviewed promptly upon receipt to verify that all transactions were made by authorized parties; any transactions made by unauthorized parties should be reported to the appropriate financial institution, card issuer or biller.

• Transaction receipts should be saved and compared to statements to ensure that unauthorized charges have not been added. Any transactions made by unauthorized parties should be reported to the appropriate financial institution, card issuer or biller.

• Incorrect transaction receipts should be voided.

• Blank transaction receipts should not be signed. Draw a line through any blank spaces above the total on any transaction receipt that is to be signed.

• Statements, bills and transaction receipts that are to be discarded should be eliminated securely, for example by shredding, and should not be discarded in a readable form.

• Financial institutions, card issuers and billers should be notified in advance of a change of address.

Use Social Media Securely
• The highest available level of privacy and security settings should be selected and activated on any social media site.

• No information that can be used to compromise information security should be viewable on any social media site. Such information includes the names of financial institutions, card companies, commerce websites, Internet service providers, utilities and wireless carriers with which you have accounts. This also includes personal financial information, passwords, phone numbers, email addresses, addresses and dates of significance (for example, birth dates and anniversaries).

• Accept only known and trusted individuals into your social network.

• Do not allow social media sites to scan your address book.

Monitor Credit Accounts
• Credit accounts and reports should be monitored regularly. Any unauthorized or suspicious activity should be reported promptly to the appropriate financial institution, card issuer, local law enforcement agency and the Federal Trade Commission (877-438-4338, or online at www.consumer.gov).

• As a precaution, you may choose to place a fraud alert on your credit file. A fraud alert will notify you before unauthorized third parties open new accounts in your name or charge existing accounts in your name. This can be done at no charge to you. To receive fraud alerts, contact Equifax® (800-525-6285), Experian® (888-397-3742) or TransUnion® (800-680-7289).

Connect With Us
For more information about Retail Online, Business Online or other online banking solutions from Fiserv, or if you have further security-related questions, please contact your account manager, call us at 800-872-7882 or visit www.fiserv.com.
About Fiserv

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, right now.