Best Practices Guide

fiserv.

Risk Management and Remote Deposit Capture

The image-based deposit capture revolution has introduced dramatic efficiencies, but also risk factors requiring financial institutions to utilize additional monitoring and management procedures to ensure optimal performance and security.

April 2015

Contents

Remote deposit capture (RDC) offers financial institutions innovative solutions that attract new accounts and offer added convenience for customers. It also carries with it risks that must be recognized and managed. This document offers guidelines and best practices pertaining to RDC technology and regulatory compliance, furnished as part of our ongoing commitment to provide you with tools, information and services that will help your financial institution operate as securely and efficiently as possible.

The Federal Financial Institutions Examination Council (FFIEC) has in recent years issued a series of guidances to aid financial institutions in managing risk in this new environment. Viewing them both individually and as a whole, this paper describes key areas of the federal guidelines pertaining to RDC risk management and Internet banking authentication, focusing especially on implications for account and item processing.

Today's financial services providers expect more and better deposit capture capabilities, including remote and mobile access, consistent image quality, duplicate detection, fraud protection, courtesy amount recognition, legal amount recognition, remittance processing and ACH conversion. These remote deposit capture capabilities can now be delivered economically across all touchpoints, while reducing risk to levels well below those associated with traditional paper deposits.

Risk Management and Remote Deposit Capture

Federal Guidance Relating to Remote Deposit Capture

In January 2009, the FFIEC issued guidance, Risk Management of Remote Deposit Capture, (hereinafter, the "2009 Guidance") to financial institutions regarding remote deposit capture processes, policies and technologies. The guidance states that when properly managed, remote deposit capture can reduce processing costs, support new and existing products by financial institutions, and improve customers' access to their deposits. However, the guidance also cautions that remote deposit capture introduces new risks in addition to those of traditional deposit delivery systems.

Because RDC solutions utilize the Internet, financial institutions also need to be aware of FFIEC guidance regarding Internet banking. In June 2011, the FFIEC issued Supplement to Authentication in an Internet Banking Environment (the "2011 Guidance") to reinforce and update the risk management framework set forth in guidance issued in October 2005, Authentication in an Internet Banking Environment (the "2005 Guidance"), regarding authentication by financial institutions offering Internet-based products and services to their customers. The supplement also updates regulatory agency expectations regarding customer authentication and layered security. Additional information about FFIEC expectations can be found on the FFIEC website at: http://www.ffiec.gov/default.htm.

In this document, we detail the FFIEC's general guidance for sound risk management, while providing an explanation of how remote deposit capture solutions from Fiserv support financial institutions' efforts to address that guidance. The intent is to help our clients, and all U.S. financial institutions, be as effective and efficient as possible in the evaluation of their remote deposit capture systems, and develop profitable strategies around its implementation.

Risk Assessment

The FFIEC recommends in the 2009 Guidance that financial institutions view remote deposit capture as a different and separate delivery system, and not simply an additional service. Prior to implementing remote deposit capture, senior management should identify and assess legal, compliance and operational risks associated with RDC deployment, and incorporate systems assessments into existing risk management processes. The 2009 Guidance also suggests taking into account the high-level descriptions of risk management processes found in:

- FFIEC Information Technology Examination Handbook: Management Booklet. This Management section of the IT Examination Handbook provides a high-level overview about management's relationship to operational and nonoperational risks, describes the structural issues associated with IT oversight, describes a process for managing technology-related risks and provides additional guidance for companies providing technology services to financial institutions.*
- FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual: Risk Assessment Overview. The Risk Assessment section of this manual provides guidance to examiners for examining a bank's BSA/AML risk profile and internal risk assessment processes. An assessment generally involves two steps: Identification of specific risk categories unique to the bank (products, services, customers, entities, transactions and geographic locations); and a detailed analysis of the data identified to better assess the risk within each of these categories.

* Note that elsewhere within the 2009 Guidance the FFIEC points to other sections ("booklets") of the IT Handbook as sources of additional useful information, including the Audit, Business Continuity Planning, Information Security, Operations, and Outsourcing Technology Services Booklets.

The 2009 Guidance also states that a financial institution's RDC risk assessment should include a determination of the risks to the security and confidentiality of nonpublic personal information consistent with the Interagency Guidelines Establishing Information Security Standards. These guidelines summarize the obligations of financial institutions to protect customer information, illustrate how certain provisions of the guidelines apply to specific situations, and provide lists and resources helpful in assessing risks and designing and implementing information security programs.

Legal and Compliance Risks

In the 2009 Guidance, senior management is advised to identify and assess exposure to legal and compliance risks related to RDC. For example, if a financial institution accepts a deposit of check images from a customer through its remote deposit capture system, legal risk exposures may be related to the controls over the process used for image capture or image exchange, and the institution's arrangements and contracts for clearing and settling checks. When a financial institution sends the deposited items, in either electronic or paper form, to another institution for collection or presentment, it should consider the risks it takes under the Check Clearing for the 21st Century Act (Check 21 Act), Regulation CC, Regulation J, applicable state laws, and any agreements or clearinghouse rules.

The financial institution should evaluate potential risks and regulatory requirements under Bank Secrecy Act laws and regulations when designing and implementing a remote deposit capture system. The institution should consider whether and to what extent it could be exposed to the risk of money laundering activities, as well as its ability to comply with anti-money laundering laws and regulations, and suspicious activity monitoring.

Operational Risks

The 2009 Guidance states that senior management should understand operational risks and ensure that appropriate policies, procedures and other controls are in place to mitigate them, including physical and logical access controls over remote deposit capture systems, original deposit items at customer locations, electronic files, and retained nonpublic personal information. Management should assess carefully how RDC affects existing risks and mitigating controls. For example, for the various technological options, management should assess the risks associated with how and where nonpublic personal information is captured, transmitted, retained and destroyed. Management should consider the confidentiality, integrity and availability of data accessed by IT systems used by the financial institution, its service providers and customers.

A financial institution should carefully consider the authentication method appropriate for remote deposit capture customers. As stated in the Interagency Guidance on Authentication in an Internet Banking Environment, the FFIEC considers single-factor authentication, when used as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. These agencies consider transfer of deposit transaction information to represent "the movement of funds to other parties." Thus, for those systems using the Internet as a communication medium, management should implement multifactor authentication, layered security or other controls reasonably calculated to mitigate risks. Refer to the Multifactor Authentication section of this document for further information.

Information Security

Properly managed, remote deposit capture technology can reduce processing costs and accelerate availability of funds. However, it can also introduce new risks, including financial write-offs, loss of business, increased expense through exception processing and reputational risk based on service gaps or fraudulent activity. While maintaining the quality and integrity of technology resources is only one of many areas requiring careful assessment of risk, it is essential to upholding service and security expectations.

Most financial institutions can benefit from the business opportunities afforded by RDC, but each must understand the potential risks and make a determination of risk tolerance. The FFIEC guidelines state that "depending on how remote deposit capture is implemented, the financial institution's risk assessment should include its own IT systems as well as those of its third-party service providers and RDC customers."

As a provider of RDC technologies and services, Fiserv supports client efforts to mitigate the legal and operational risks related to serving customers making deposits from locations other than a bank branch. The foundation of the Fiserv risk management strategy is an extensive set of information security risk and privacy policies, standards and programs that address security management, risk management, architecture, data protection, access control, software development, monitoring and management, incident response and business continuity.

Based on this framework, policies and procedures have been developed to standardize information security activities in areas specific to remote deposit capture technologies and item processing. Designed to meet or exceed the requirements established by the Interagency Guidelines Establishing Information Security Standards, these procedures include, but are not limited to, the following:

- Access controls on customer information systems, including controls to authenticate and permit access to only authorized individuals
- Controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means
- Physical access restrictions at locations containing customer information, such as buildings, computer facilities and record storage facilities to permit access to only authorized individuals
- Encryption of electronic customer information in transit and at rest when deemed necessary and appropriate
- Stringent pre-employment screening and segregation of duties for employees with responsibilities for or access to customer information
- Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems
- Response programs that specify actions to be taken when access to customer information systems by unauthorized individuals is suspected or detected
- As required under applicable laws, prompt client notification if the personal information of the client's customer(s) was, or is reasonably believed to have been, acquired by an unauthorized person
- A disaster recovery plan to protect against loss of or damage to customer information due to potential environmental hazards, such as fire and water damage or technological failures
- Appropriate controls designed to ensure the proper disposal of "consumer information"

Information Privacy

Part of system security is upholding the privacy and integrity of personal information throughout deposit activities, regardless of the processing channel used. In the context of remote deposit capture, direct control over the origination point of the deposit activity the home or business location, for example is outside the means of the financial institution. However, once data has been entered or a check has been imaged into a supported technology, it then enters the operational domain of the institution and any stakeholders in the processing chain, including third-party providers.

Fiserv understands the importance to both the financial institution and the end user of continually assessing risk and ensuring the protection of personal information throughout the transaction life cycle and as long as data is retained within the system. The processes outlined below adhere to applicable laws and regulations while accounting for the best interests of our clients and their customers:

- All personal information is evaluated for the level of sensitivity, and critical information resources are protected.
- Fiserv protects the confidentiality, privacy, integrity and availability of personal information in all forms whether created by Fiserv or entrusted to us by our clients, partners or suppliers.
- Fiserv protects the integrity and availability of processes and systems handling personal information.
- Employees having access to or controlling personal information are accountable for their actions.

- Employees compromising Fiserv information security or interfering with or refusing to cooperate in an investigation of an actual or suspected violation of this policy are subject to corrective actions, up to and including termination of employment, as appropriate.
- Fiserv educates employees on the need for, methods of and responsibility for information security and privacy. The level of training provided is based on the employee's authority over and access to personal information.
- Fiserv prepares for continuity of business operations in the event of an emergency situation.
- Fiserv fulfills its contractual obligations to clients and business partners with regard to information security and privacy.
- Fiserv has an established formal process for responding to security and privacy incidents.

Other Legal and Operational Risks

In addition to these information security and privacy concerns, operational activities can increase risk for the financial institution. Channel risks outlined in the FFIEC guidelines include faulty equipment and inadequate procedures or training that could lead to inappropriate document processing, poor image quality and inaccurate electronic data. Fiserv regularly monitors the industry, communicates information to clients about scanning equipment that is compliant with its technology and processing systems, and offers consultative resources, including through our partner Beavercreek Marketing. Refer to the RDC Training for Customers section of this document for further details.

Technology policies comprise only part of a full risk assessment strategy. Information security, data protection and error reduction also require careful evaluation of human resources. Fraud related to deposit activity, including check alteration, forged endorsements and counterfeiting, are not exclusive to RDC. Some types of fraud can be mitigated by technology. For example, image ATMs enabling remote deposit capture can reduce empty envelope fraud at the ATM.

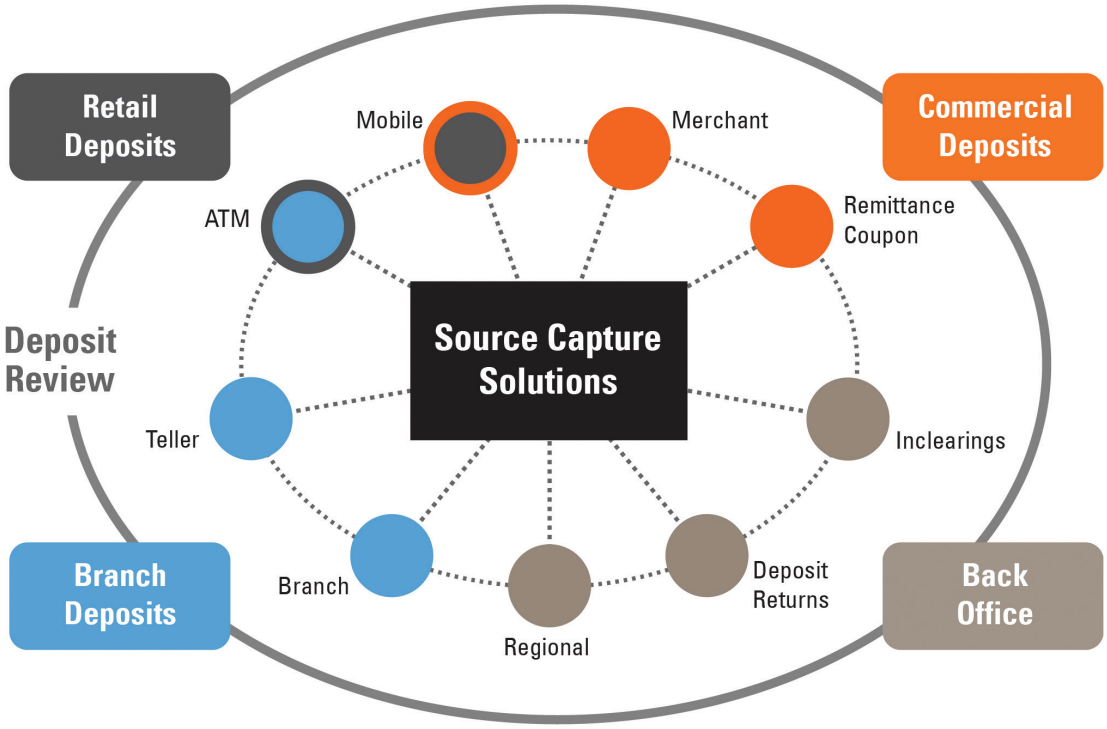
But FFIEC guidance reminds us that some threats can be more difficult to detect in a highly automated, multichannel deposit system. One of these is the opportunity for duplicate items to enter the system, either inadvertently or as a deliberate fraud. A strategy of using one common solution set (such as the Fiserv remote deposit capture product suite known as Source Capture Solutions®) to capture all deposits from a branch, business, or a customer's home or office significantly reduces acceptance of duplicate items. For example, if a consumer deposits a check using a smartphone and then another family member takes that same check into the branch, the item is immediately flagged as a duplicate and stopped from entering the system.

While financial institutions cannot fully control the activities of customers' employees, they can assess the risk associated with companies and individuals expressing interest in remote deposit capture prior to authorizing use of those services. In addition, customer activity should be monitored on a regular basis to identify and manage higher-risk RDC users. To facilitate monitoring customer activity across all channels, Fiserv includes Deposit Review as an integrated component of Source Capture Solutions. Refer to the Measuring and Monitoring section of this document for further details.

As a provider of financial technologies and associated services, Fiserv maintains policies that address risks, including those pertaining to human resources that may have access to client and customer assets or information. Throughout employment, Fiserv engages in security screening, awareness and enforcement practices including but not limited to background checks, annual distribution of information policies and physical access restrictions.

Moreover, the Fiserv Enterprise Risk & Resilience group, under the guidance of the Chief Risk Officer, has established an Enterprise Risk Assessment program. All Fiserv business units participate in the program and create annual assessments that identify critical information assets relevant to services provided to clients, determine risk profiles related to primary risk categories, quantify inherent and residual risks, summarize existing applicable controls, and drive the ongoing remediation and mitigation plans for identified risks.

FFIEC guidelines address, and Fiserv supports, these processes and procedures that help financial institutions carefully assess risk as a key component in planning for



Remote Deposit Capture is a multifaceted, multichannel solution which touches every aspect of a financial institution's operation. RDC also carries with it inherent security risks which must be recognized and managed.

the provision of remote deposit capture services. This requires careful consideration of customer engagement strategies and third-party vendors to ensure that all aspects of the program meet necessary legal, operational and regulatory compliance requirements.

Multifactor Authentication

According to the 2011 Guidance, financial institutions should perform periodic risk assessments and adjust their customer authentication controls as appropriate in response to new threats. As regulatory guidance around vendor management increases, financial institutions should proactively assess their critical suppliers.

Customer Authentication for High-Risk Transactions

Financial institutions should implement increasingly robust controls as transaction risk levels increase. The FFIEC recommends that institutions offer multifactor authentication to their business customers. Since the frequency and dollar amounts of business/commercial banking transactions are generally higher than consumer transactions, they are deemed by the FFIEC to pose a relatively greater level of risk.

Through our Source Capture Solutions, Fiserv supports Security Assertion Markup Language, or SAML, which allows for secure authentication verification from an online or mobile banking system. Authentication to Source Capture Solutions is typically achieved by first authenticating through the interfacing online banking or mobile banking product.

Layered Security Programs

Layered security can substantially strengthen the overall security of Internet-based services and be effective in protecting sensitive customer information, preventing identity theft, and reducing account takeovers and associated financial losses. Effective controls that can be included in a layered security program include but are not limited to:

- Fraud detection and monitoring systems that include consideration of customer history and behavior, and enable a timely and effective response from the financial institution

- Enhanced controls over account activities, such as transaction value thresholds, payment recipients, number of transactions allowed per day, and allowable payment windows (for example, days and times)
- Enhanced control over changes to account maintenance activities performed by customers either online or through customer service channels

According to the 2011 Guidance, layered security controls should include processes designed to detect anomalies and effectively respond to suspicious or anomalous activity related to:

- Initial login and authentication of customers requesting access to the financial institution's electronic banking system
- Initiation of electronic transactions involving the transfer of funds to other parties

For business accounts, layered security should include enhanced controls for system administrators granted privileges to set up or change system configurations, such as setting access privileges, and application configurations and/or limitations.

The Source Capture Solutions product set supports multiple security roles that enable deferred approvals from the point of capture through submission. Use of duplicate item detection and Image Quality Analysis (IQA) allow for proactive fraud detection and reduced overall risk from all capture channels. For control over daily transaction, single transaction and single item values accepted at a customer or single-user level, values are determined by the overall risk factors associated with the RDC user.

Support for SAML user authentication integration offers additional security where user profile information maintenance is performed outside of the application via the online banking or mobile banking application. Fiserv provides automated duplicate item detection, item image quality analysis, limits on deposit dollar amounts and on the number of deposits, and advanced reporting to identify anomalous transactions. Additionally, defined security roles and permissions control functions allowed for individual users.

Mitigation and Controls

Once it has been determined that remote deposit capture is to be offered and an acceptable risk tolerance has been established, risk management strategies should be developed. The FFIEC provides a policy framework that incorporates guidance on customer due diligence, vendor due diligence, training, contracts and business continuity.

Customer Due Diligence and Suitability

Knowing your customers and monitoring them regularly are key factors in minimizing risk. Because activities at the origin of the deposit collection process are not under the direct control or oversight of the financial institution, the FFIEC encourages the establishment of risk-based guidelines to qualify customers, and suggests that Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) programs can form the basis for eligibility. Just as institutions and vendors must uphold customer trust when processing and using information, RDC requires an additional level of trust in the customer to accurately and ethically initiate deposits. Fiserv can assist with these responsibilities by enabling RDC clients to set different roles and limits for end users to reflect varying levels of trust.

Vendor Due Diligence and Suitability

The FFIEC states that "financial institutions that rely on service providers for RDC activities should ensure implementation of sound vendor management processes." Outsourcing RDC can be an effective and efficient means of deploying the service, with operational and cost benefits to the financial institution. But dozens of vendors compete in today's marketplace, and vendor selection is about more than technology and price. A partner in RDC should understand an organization's tolerance for risk and have the capabilities and product offerings to deploy a solution in accordance with individual business strategies and risk thresholds.

As a leader in item processing and remote deposit capture technologies, Fiserv welcomes the opportunity to engage in financial institutions' evaluation processes, describing our policies and procedures, pointing to successful audits, and demonstrating the strengths of our consumer, merchant and branch solutions.

RDC Training for Customers

Fiserv recognizes the value of comprehensive training programs for financial institution employees, their customers and other end users on the proper and secure use of technology solutions. Fiserv has partnered with Beavercreek Marketing to develop a complete marketing and training programs for mobile banking/mobile deposit, merchant and consumer RDC deployment.

These programs can be extremely helpful in successfully deploying any of the Fiserv remote deposit capture solutions, and are available in printed and online formats through the Online Education Center. Each deployment kit includes a risk management worksheet used to evaluate potential users of RDC technology to help ensure they meet acceptable risk standards. Visit bankall.com/ for more details.

Contracts and Agreements

Contracts and agreements define the partnership between financial institutions and other stakeholders engaged in the implementation and maintenance of RDC technologies and associated business processes. Fiserv has worked with many financial institutions and has the expertise needed to develop mutually agreeable documentation of processes, procedures, roles, responsibilities and obligations.

Contracts and agreements also define the partnership between financial institutions and their customers. Fiserv has partnered with Beavercreek Marketing to offer sample customer agreements for financial institutions to review and modify for their specific needs. Particularly helpful for institutions new to RDC, these agreements include key provisions that help customers understand their rights and obligations.

Business Continuity

Once an RDC process is initiated, risk shifts from evaluative criteria to service obligations. According to the FFIEC, "The financial institution's business continuity plan should address RDC systems and business processes, and the testing activities should assess whether restoration of systems and processes meets recovery objectives and time frames." As a business-critical partner to thousands of organizations requiring superior levels of performance and reliability, Fiserv has developed a comprehensive business continuity plan in accordance with its information security risk and privacy programs, and industry best practices:

- Business continuity plans restore operations to required levels of service without increasing the level of security exposure.
- Business continuity plans are regularly tested.
- Contingency and business resumption planning are addressed in coordination with information security programs and policies.
- Data backups are stored off-site at a secure location to minimize the impact of and loss of data due to a natural disaster.

Measuring and Monitoring

The FFIEC provides guidance on the monitoring and measurement of risk management programs. System reports from remote deposit capture solutions can provide a wealth of information to financial institutions, including data related to performance and efficiency, compliance, fraudulent activity and customer quality. Deposit review functionality is desirable, offering customizable risk reporting and duplicate item identification.

Financial institutions using Source Capture Solutions from Fiserv can use Deposit Review to examine deposits across one or multiple points of capture, flagging deposits for review based on customizable risk factors. For example, if a change is made to a deposit, the system delivers a notice to the customer via email or a secure message from within the application. Reports are generated and tailored for functions such as customer billing, workflow management, customer service and quality control. Likewise, if an item is deposited remotely at a merchant capture site and then inadvertently (or deliberately) brought into the branch, Deposit Review identifies that item, reducing the chance of duplicate items entering the system.

Tools are also available to help organizations measure and monitor risk. Fiserv partners with Beavercreek Marketing to offer an Electronic Banking Risk Assistant that helps simplify the complex and time-consuming

task of completing risk assessments for each of your online banking solutions. Users respond to the survey questions provided, and assign a risk rating based on the Likelihood of Risk, and also the Consequence of Risk. The survey questions and responses provide a useful guide for determining your own risk ratings, helping the financial institution comply with the FFIEC's 2011 Guidance, Supplement to Authentication in an Internet Banking Environment.

New Technology and Research

With the availability of new mobile technologies, mobile banking from smartphones and tablets is on the rise. Many financial institutions already offer applications that let customers check balances, transfer funds and make payments from their mobile devices. Mobile check deposits are the logical next step, and promise to attract a significant number of new mobile banking users.

Mobile Deposit

Products like Mobile Source Capture™ from Fiserv enable the smartphone's camera to take a picture of the front and back of each check and submit the images electronically to the financial institution for processing, clearing, settlement and posting. Checks can be deposited individually, as they are received, reducing the potential for checks to be lost or stolen.

Fiserv and other vendors offer financial institutions the opportunity to implement pilot programs for mobile capture, in order to better understand both compliance and operational risk, and formulate appropriate methods to manage it. Running a well-planned and documented pilot with a select group of customers is highly recommended. By following standard risk guidelines for customer eligibility and usage, the mobile capture channel presents no more or less risk than any other RDC channel.

Research Shows RDC Losses Remain Low

In its report "State of Remote Deposit Capture: All About Mobile" (January 10, 2014), the research and consulting firm Celent confirms that RDC fraud loss in the industry continues to be low. While it remains essential for financial institutions to follow industry guidelines and remain vigilant, the report shows that 21 percent of banks surveyed suffered any kind of loss attributable to remote deposit capture, with the majority of loss occurring at larger banks with more than $50 billion in assets. Of those that had some loss, duplicate presentment was the cause of a full 70 percent of all reported incidents, and 40 percent involved a deposit being made twice through separate channels at the same financial institution.

Another Celent report, "Evaluating the Enterprise-Wide Compliance Vendors," issued in February 2012, profiled and ranked 22 providers of solutions for anti-money laundering and anti-fraud. It underscores the fact that the marketplace offers many end-to-end solutions that support the full scope of compliance, and every phase of the banking process (Fiserv was shown to serve more financial institutions than any other provider profiled).

Connect With Us

For more information about remote deposit capture or our Source Capture Solutions, 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 now.

fiserv.

Fiserv, Inc.
255 Fiserv Drive
Brookfield, WI 53045

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

412-15-25425-COL 04/15