Getting ahead of risk:
How to attract and serve commercial clients without burdening your back office

With limited resources and technology, community-focused financial institutions (FIs) must leverage automation to help them create efficiencies around fraud and risk management, so that they can better serve corporate clients. The right technology can help FIs avoid back-office bottlenecks and manage fraud more effectively—while also allowing them to offer a level of service that lets them compete with larger FIs for business accounts.

Put another way, FIs need automation to grow. It’s as simple as that.
Introduction

How the fraud landscape drains resources and hampers growth

Check and ACH fraud combined account for nearly $10 billion in losses annually. With only a routing number and an account number, cybercriminals can do a lot of damage—particularly to businesses with growing numbers of transactions but no way to detect fraud at scale. FIs that want to serve businesses need solutions that assess risk and manage fraud for their customers. But unless their solutions have the ability to scale, the operational lift required to manage fraud can quickly overwhelm both the FI and its customers.

This strain on resources not only limits community FIs’ ability to attract and serve large commercial accounts, but also limits their ability to onboard new business customers without overwhelming their back-office and support staff. This makes growth problematic at best.

In the following report, we’ll outline the growing need to compete for commercial accounts, as well as describe technology that can help community FIs serve businesses efficiently and effectively without over-burdening their back office.

Places to learn about industry fraud:

- National Automated Clearing House Association (NACHA)
- Regional Payments Associations (RPA)
- Federal Trade Commission (FTC) reports
- Consumer Fraud Reporting
- FBI.gov and USA.gov scam lists
- National Association for Financial Professionals (AFP®)
- Regional Associations for Financial Professionals
Part I. The need to compete

According to a Harvard report, “community banks’ share of U.S. banking assets and lending markets has fallen from 41 percent in 1994 to 22 percent today, while the market share of the top five largest banks has more than doubled from 17 percent to 41 percent.”

To weather this downward trend in market share, community FIs may consider diversifying out of consumer lending and into business products and services. Many, though, feel unprepared to manage the complexity associated with larger commercial accounts. But, despite limited resources, community FIs can support advanced business services—with the help of the right technology.

Risk and fraud management solutions are a perfect example of the technology gap often facing community FIs. Large institutions have robust offerings that address risk and fraud; to compete for business customers, community FIs need comparable offerings. To compete at the highest level, risk and fraud management tools have to be:

- **Automated** – Community FIs have to do a lot with a little. The more processes they can automate, the more time they can spend serving account holders. Automation can also help reduce the errors potentially created in manual processes, as well as create audit and reporting trails crucial to compliance.

- **Scalable** – A solution that enables growth is only as good as its ability to scale with the growth it creates. Even with only moderate FI/customer growth, the constantly increasing incidence of fraud makes detecting and managing it a heavy lift. The ability to easily scale fraud mitigation efforts will be crucial in the years to come.

- **Comprehensive** – To compete against big banks, half-measures won’t do, and piecemeal solutions cobbled together from multiple vendors end up costing more and creating more hassle than value to the FI or their customers. Many times, for example, check and ACH positive pay require additional work for the back office in terms of user setup and configurations. Consolidating functions within a single system can save time, money, and trouble.
Part II. A better experience

To date, non-financial brands like Amazon and Netflix have been setting the bar high for seamless, intuitive user experiences. FIs that aren’t meeting these expectations don’t inspire confidence. They appear out-of-date, their end users are likely frustrated, and they’ll find it increasingly difficult to compete with more tech-savvy FIs.

The often-heard counter argument to this point is that slick user experiences fall within the purview of consumer-targeted technology; the expectations around commercial solutions—including fraud and risk management tools—are different. This may have been true a few years ago, but the expectation gap is closing. Commercial users know what consumer experiences are like from their daily, personal interactions with best-in-class providers—and today they’re less forgiving of subpar usability in their commercial solutions.

At the end of the day, commercial solutions don’t have to be piecemeal; they should be comprehensive, integrated, and easy to use. They should be user friendly and aligned with need and expectations alike.

This is true of the experiences both within the FI and those they offer to their account holders. Even if a solution isn’t customer facing, if it has subpar usability, it will hurt productivity and possibly require additional or on-going training.

In the following section, we’ll look at specifics, giving examples of efficiency gains and other ways that that commercial risk and fraud solutions can create better experiences, while also saving time, money, and trouble.

Part III. The cost of ignoring your back office

In January of 2018, Hawaii was alerted to incoming ballistic missiles. It was not, they were told, a drill. For half an hour the state believed it was under attack, until it was revealed that the intended communication should’ve indicated it was only a test of the system.

The culprit was clumsy technology. The choices for “test alert” and “real alert” were too similar in the warning system’s interface.

Translating this incident to FI operations, a poorly managed back office and inelegant technology can cause problems with serious fallout. An FI may not be able to put the fear of a missile attack into its account holders, but they can just as easily fail to spot fraud, make transactional mistakes, or fail to maintain compliance if their back-office tools are antiquated, clumsy, or confusing.

This makes it difficult to maintain the status quo, much less compete and grow.

The painful truth is that investing only in customer-facing-solutions, while ignoring back-office upgrades won’t do much good in the long run. Everything starts with the inner culture and back office. The 2018 World Economic Forum report by Bain & Company suggests that only about 1 percent of the over a trillion dollars invested in transforming digital banking will achieve the targeted return on investment.2
Additional research by McKinsey & Company suggests that upgrades to back-office technology and increasing automation can result in an improvement of more than 50 percent in both productivity and customer service.³

Finally, the Boston Consulting Group reports that, in recent years, global banks’ revenues have remained flat, while their costs have increased by nearly 10 percent. Their answer to this trend, which appears to be ongoing, is in part to digitize and simplify products, services, and their underlying processes.⁴

If FIs want to compete in the digital landscape, grow, and scale their workload effectively, they need better tools, processes, and workflows in their back offices.

Additional research by McKinsey & Company suggests that upgrades to back-office technology and increasing automation can result in an improvement of more than 50 percent in both productivity and customer service.

Part IV. Streamlining fraud and risk management

Now that we’ve covered some reasons why it’s crucial to create back-office efficiency, let’s talk about how. In this section, we’ll discuss best practices and technology that can streamline risk and fraud management processes to save your FI time, money, and trouble.

Automate, integrate, and get comprehensive

The first step to streamlining your back office is to replace as many obsolete manual processes as possible. Trying to handle file mapping for check positive pay with an Excel spreadsheet, for example, is a laborious task, with a lot of back and forth between the client and your FI. Manual aggregation of originator data for annual risk reviews is also a difficult, time-consuming, and piecemeal process.

These kinds of tasks simply eat up too many resources. And manual processes aren’t just slower, but they also invite error and create little or no audit trail. They limit your ability to generate reports and, because they exist in isolation, with no real points of integration, they do nothing to contribute to a cohesive, holistic view of fraud or risk.

While no single system can handle all of your back-office needs, combining a wide array of functionality under the same login and system can save money and streamline operations. The ACH and check positive pay system we referenced in Part I is a perfect example of this kind of comprehensive solution as it relates to transaction management and fraud detection. And a risk management system that oversees and automatically aggregates all kinds of transactions and originator activity can also make risk reviews faster and easier.
An efficient back office should have tools that include:

1. A combined check and ACH positive pay solution that features:
   - Full account reconciliation
   - Advanced reporting
   - Reverse positive pay
   - Payee match functionality that compares payee names and check images
   - Data mapping that lets banks accept check file formats native to their customers’ accounting systems
   - Automatic generation of ACH return transaction posting files
   - Automated notification emails and text messages to clients when exceptions are present

2. A comprehensive risk management solution.

FIs need streamlined ways to carry out comprehensive ACH and RDC risk assessments in order to better manage exposure and ensure compliance—including the ability to monitor and validate all ACH origination activity. Many online banking systems do include some rudimentary origination rule validations. But a more effective payments monitoring system requires a robust and highly customizable rules engine with pre-authorized account list validation and dollar limit checks based on the file or originator. These validation checks should be available to all channels—whether an ACH file is submitted through an online banking platform or through an alternative means, like an SFTP server.

A comprehensive risk management portal should also be able to generate extensive reporting in a user-friendly manner. Some of the kinds of reporting FIs need to adequately handle risk assessments for commercial clients include:

- Activity analysis by day or month
- High-risk originator monitoring
- Transaction analysis by SEC code
- Volume reporting
- Exposure reporting
- Exception reporting
- Trending charts and graphs
- Returns analysis

Traditionally, the risk assessment process is very labor intensive for financial institutions. The amount of work involved makes it difficult to grow and add a large number of ACH or RDC business customers—unless the FI has a way to streamline the assessment process. To effectively scale, a risk assessment solution should provide the following efficiencies and features:

- The consolidation of data from disparate transaction channels should be automated. (DDA, Savings, COD, Loans, RDC, and Wires)
- The user interface should provide a concise, easy-to-interpret view of the total relationship, including the details of the most recent reviews and when the next review will occur.
- The process should be paperless, to avoid wasted resources and manual errors.
- The tool should incorporate a workflow for altering/approving changes to exposure limits based on risk assessments.
- The solution should be customizable and flexible. Each FI approaches assessments a little differently, so the risk review tool should allow the FI to choose data sources and elements based on their needs and processes.
Fraud Management and Risk Management working together:

Combining the fraud detection of an automated, comprehensive positive pay solution with the customer-level details of a holistic risk management tool can help FIs address exposure while streamlining their operations and reducing loss.

The importance of integration

• A seamless, single sign-on within your digital banking interface saves time and creates a better customer experience.
• Integration with teller systems can help keep your frontline engaged in fraud detection.

Conclusion

What would your financial institution be able to accomplish if you were able to reduce the time spent on fraud and risk management? To compete, community FIs need to be confident in their ability to scale their services as their customer base grows in size and complexity.

Fraud is unfortunately here to stay, and risk goes hand-in-hand with offering and managing financial services. The ability to effectively handle these factors can make or break FIs’ ability to attract and serve commercial clients. With increasing competition and shrinking market share in the consumer space, FIs hoping to grow should consider extending additional business services and competing for larger commercial accounts.

With the right technology, it’s not only possible to manage your existing business accounts better, but it’s also feasible to grow and serve larger clients without adding a significant burden to your back office.

About Centrix Solutions

Centrix Solutions, a Q2 company, provides financial institutions with best-in-class products that detect fraud, increase operational efficiency, and support compliance. Our team provides in-depth knowledge and has vast experience in developing and delivering quality solutions that help FIs automate and streamline risk assessments, treasury management, compliance, and more.
Sources


Appendix

Learn more about fraud in the financial industry:

www.nacha.org
www.nacha.org/members/regional-payments-associations
www.ftc.gov
consumerfraudreporting.org
www.fbi.gov/scams-and-safety/common-fraud-schemes
www.usa.gov/common-scams-frauds
www.afponline.org
www.afponline.org/about/learn-more/regional-associations
Biography

Steve Bartels
AAP, Senior Director of Solutions Consulting, Centrix Solutions, Q2 Software

With almost 30 years of experience in the financial software industry, Steve Bartels has led high-performing teams, managed complex projects, and consistently exceeded customer expectations. He also leads the Centrix Solutions Consulting team, providing clients with a wealth of industry expertise, as well as technical and product knowledge. Mr. Bartels holds a Bachelor of Science in marketing from the University of Nebraska.