Quatrro
Beyond the existing
PROCESSING SERVICES

Toward a Strategy for Enterprise Risk Management

Building a Foundation to Mitigate Fraud in a Cross-channel Environment

Consumers today enjoy many choices from their financial services provider thanks to a deep product suite offered through multiple distribution channels. Credit unions and banks realize that service is key to retaining hard-won business. And there is a growing desire to expand products and serve consumers in non-traditional means to deepen those relationships. One only needs to consider the growth in electronic banking through tablets and smartphones to realize that service is king. While product and channel delivery is expanding, financial institutions run the risk of weakening the chain that binds and protects their enterprise. Criminals are increasing their attacks on both traditional and emerging bank channels making it imperative to provide real-time enterprise-wide fraud protection.

Traditional Services Will Remain Vulnerable

History proves that the financial services industry has not completely eliminated fraud from traditional banking channels. And, it never will. The industry must continuously evolve with the criminals to tighten the noose on fraud. Consider the following examples:

ACH/Wire. Traditional services such as ACH and wire transfers continue to remain vulnerable to fraud. Consider the recently reported case whereby a criminal deployed a distributed denial-of-service attack on a bank draining up to $2.1 million from the

institution. Security researchers at Dell SecureWorks said that a short-lived DDoS attack against a financial institution could be an indicator of an unauthorized wire transfer. According to the Financial Services Information Sharing Analysis Center (FS-ISAC), "The DDoS attacks were likely used as a distraction for bank personnel to prevent them from immediately identifying a fraudulent transaction, which in most cases is necessary to stop the wire transfer."

Checks. Being one of the oldest financial instruments, checks are no stranger to fraud. These contemporary instruments continue to suffer from growing fraud despite their decline in use. According to an Ernst & Young study reported by the National Check Fraud Center, over 500 million checks are forged annually, with losses totaling more than $12 billion. Consider the recent case involving Saquib Khan who owned numerous delicatessens on Staten Island. Near bankrupt and at risk of losing everything, he wrote hundreds of forged checks to himself and then deposited them in multiple banks under his name or his business name. The fraudulent checks totaled $82 million – most, but not all, was recovered. To this day, it is considered to be one of the largest check-fraud schemes in the U.S.

Card Payments. On the other side of the payments spectrum are credit and debit cards – regardless of whether criminals use sophisticated or unsophisticated methods. The U.S. currently accounts for 47% of global credit and debit card fraud even though it generates only 27% of the total volume of purchases and cash, according to The Nilson Report. Payment card fraud losses totaled $3.56 billion last year in the U.S. from all general purpose and private label, signature and PIN payment cards. Consider that most financial institutions use rules-based monitoring to block suspicious and fraudulent transactions. Regrettably, fraud leakage still occurs in significant amounts.

Mortgage Fraud. Although the exact amount of money lost to mortgage fraud is difficult to pinpoint, the Federal Bureau of Investigation estimates that that more than $10 billion in loans are originated each year with fraudulent application data. But, fraud does not cease once the loan has been booked. Banks and credit unions are still at risk. Consider a bank employee that helps a friend by illegally altering his mortgage rates or terms so his home does not go into foreclosure.

Next Generation Services Offers Uncertain Fraud Outlook

Next generation banking channels and services are coming into focus. Growth in banking through smartphones and tablets is up with advances in mobile payments and Remote Deposit Capture (RDC) gaining traction. In a recent survey of financial industry vendors and service providers, Boston-based Celent LLP found that 80% of financial institutions are planning or considering a mobile RDC solution. And with more than 50 million Americans expected to do mobile banking by 2015, according to Forrester Research, it should be no wonder that mobile RDC is becoming "table stakes" for financial institutions of every size. These upward trends in next generation services are intriguing, but one should have guarded optimism.

Mobile Banking. Mobile banking introduces a great opportunity to improve the customer experience through anywhere, anytime banking. However, as financial institutions introduce this new channel to their customers, they need to ensure the risks don't outweigh the rewards. Consider that a credit union is likely to have historical check transactions on file from which to build fraud rules that flag out-of-trend behavior. Because mobile banking and payments are relatively new, the storehouse of behavioral data is not as mature. Financial institutions need to better understand how their customers are using their smartphones and tablets for banking. Building that storehouse of transaction data will help banks reduce their fraud exposure when blended with an effective rules-based platform.

Remote Deposit Capture. Mobile-based RDC is a classic case of providing

convenience all while wrapped in a very elegant and consumer-friendly application. One can simply take a picture of their check within their bank application and send for deposit anytime, anywhere. However, fraudsters are finding opportunities in duplicating these RDC checks. In a recent incident, a group of Russian criminals broke into an online check-image database, reproduced 3,000 checks and sent them to money 'mules' for deposit, after which they wired the proceeds to themselves. Approximately 1,200 U.S. bank accounts were stripped of $9 million.

Caution with Point Solutions

The reality for financial institutions is that fraud cannot be totally eliminated from the equation. It must be a calculated cost of doing business in an ever expanding and complex banking environment. When fraud does occur the expected usually happens – a bank representative will find a stop-gap solution for that specific problem irrespective of the broader business implications or threats from outside his/her area of responsibility. These are called point solutions.

Not Comprehensive. Point solutions are highly targeted solutions that address one specific problem. For example, suppose a credit union is experiencing a sharp spike in the number of 'on-us' fraudulent checks. They may look for a check image fraud solution to solve for that problem. At the same time, the credit union might also notice a number of unusual ACH routing number changes for large commercial accounts. That individual may seek out an ACH fraud solution. The end results are two vendor relationships to manage (along with different SLAs); two separate products to manage; two separate invoices to process each month; two different tracking and reporting systems to manage; and no scalability in price.

Can be Costly. Small to mid-size financial institutions are at a disadvantage with point solutions. While fraud occurs across the industry, the ability for small to mid-tier financial institutions to cost-justify more expensive point solutions can be difficult to rationalize. While smaller institutions may not have high volumes of fraud to solve for, they are still vulnerable. And, it is in their best interest to find a bundled service as opposed to one-offs to solve for fraud breaches. This approach saves money and provides superior protection. However, larger institutions are likely to have an overabundance of point solutions with little cross-pollination to other departments. Overlaps are likely to occur whereby one department has a solution that another department could use but is not aware of. Consolidation is key.

Real-time Cross-channel ERM is Here

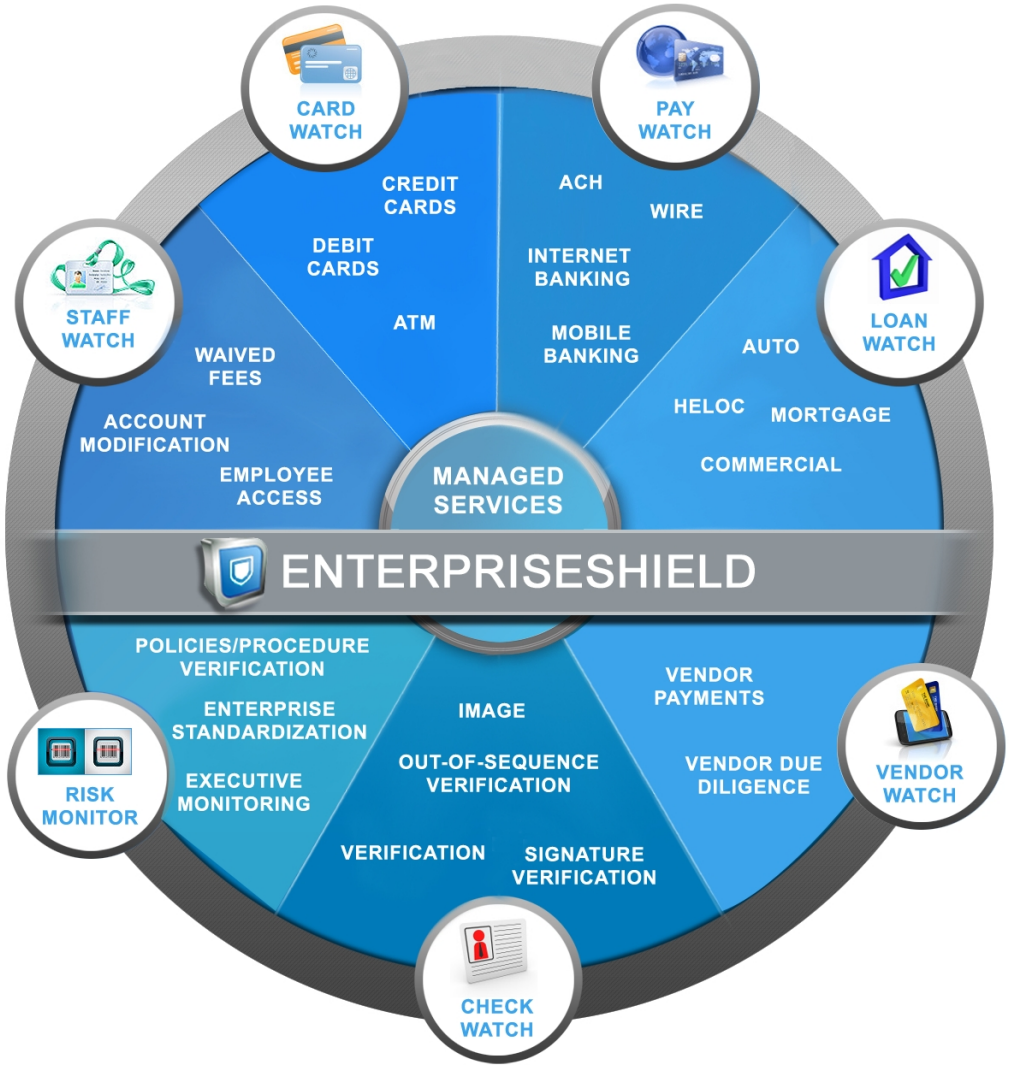
Essential to the concept of an Enterprise Risk Management (ERM) platform is the understanding that fraud attacks are rarely in silos. Criminals are increasing their attacks on both traditional and emerging financial services through multiple entry points making it difficult to manage with point solutions. Banks and credit unions need a comprehensive approach to controlling their risk. Having the ability to see all potential threats in a cross-channel environment from one single case management platform is ideal. You have the ability to see trends, analyze your fraud exposure, and make key business decisions without having to cobble together various unrelated reports. It's faster and more effective to have one single view.

Quatrro Processing Services has recently launched a new real-time ERM platform called EnterpriseShield. This is a cross-channel monitoring service built upon 7 distinct rules-based modules – all of which capture the most important and highly used banking channels. These modules protect against card fraud, ACH and wire fraud, check fraud, ATM fraud, loan fraud, internet banking fraud, internal staff fraud and much more. From one single platform a credit union or bank can provide an important 'lock box' across their enterprise. Underpinning these modules is one software program that ties the rules (modules), case management function, and reporting into one single view.

EnterpriseShield provides an effective case management dashboard for supervisors to review, assign and work fraud cases – regardless of what channel they are sourced. Targeted rules help assign a priority so you are working the most important cases first. For example, a $10,000 suspicious ACH alert would receive a higher priority than a $50 suspicious debit card alert. This allows you to assemble a cross-functional team to resolve the most important breaches first – an advantage over point solutions where the activity resides in silos.

and customized reporting. Sample reports include: financial reports, audit reports, Board reporting, loan production and portfolio analysis, fraud analysis and transaction analysis. With DataMiner there is no need to maintain your own Excel reports. Since incoming data is real-time your reports are in real-time. DataMiner turns data into meaningful and actionable business intelligence.

EnterpriseShield has been designed to be a cost-effective solution to credit unions and



Reporting and tracking is much more streamlined with our data mining feature. Every financial institution using EnterpriseShield receives access to the DataMiner tool which provides both canned

banks of all sizes, but has been constructed to be an economical alternative to other providers like Actimize and Verafin who tend to provide point solutions to the large bank market. We believe the small to mid-tier credit

union and bank markets have been historically underserved with solutions that can be financially rationalized. With EnterpriseShield, the bulk of the financial services marketplace now has access to an affordable solution.

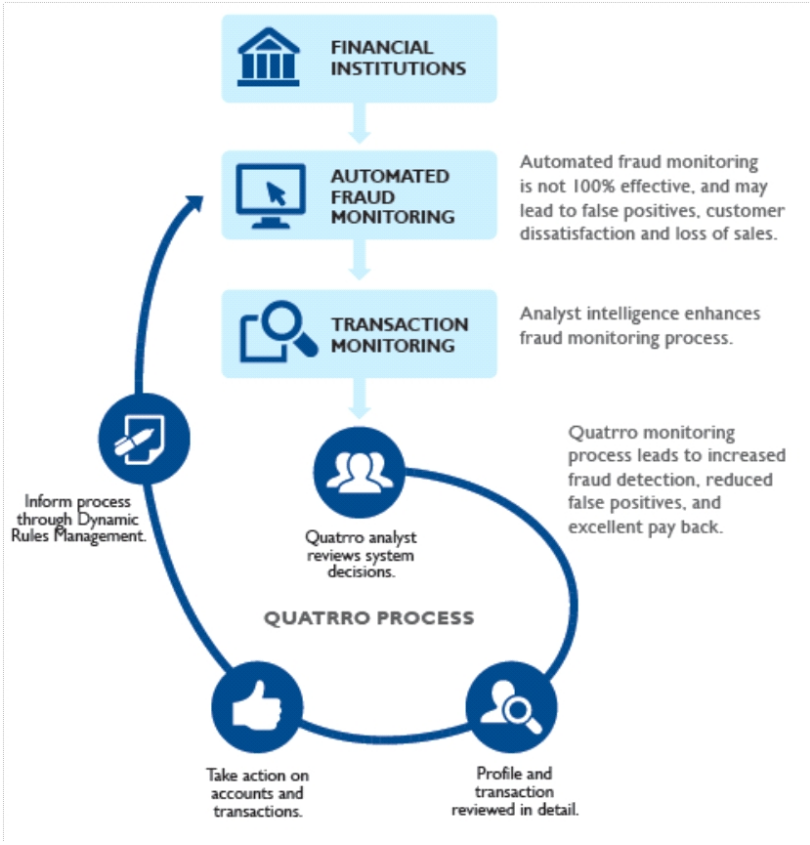
Layering is the Secret Sauce

What most banks and credit unions invest in are automated systems that detect and block fraud. But, as statistics prove, these automated solutions are not perfect and they are often not effective at standardization and monitoring across departments and product verticals. Fraud still occurs and wreaks havoc on a financial institution's customer base, its brand and its bottom line. Financial institutions should consider these solutions as a first step in a front-line defense against fraud – not as a comprehensive remedy. Until now.

Quatrro Processing Services offers access to expert fraud analysts for full-time or part-time coverage through its flag-ship Managed Services product. Consider that rules-based systems produce alerts. And, depending upon how many rules are in place, these alerts can run into the thousands within a short period of time. While these alerts are needed and useful, a financial institution must dedicate internal resources to manage the case load.

Our Managed Services offering does the leg-work via close and regular collaboration with the financial institution. We provide advice and counsel to a bank or credit union in setting up appropriate rules, monitoring alerts generated by those rules, conducting advanced analytics on flagged transactions, and refining processing parameters to stay ahead of fraud trends. With careful scoping, our Managed Services offering can be used to block suspicious transactions on behalf of the bank or credit union – eliminating potential bottlenecks and backlogs in alert case management before it gets out of hand.

Augments Internal Staff. We realize that your staff is an asset. Our Managed Services solution should not be considered as a replacement to your fraud team, but as a compliment. Our services are scalable from evening or weekend coverage, or as a compliment to your full-time transaction monitoring activities. Much like a contact center, we can turn on and off coverage as you need. Another important note is that our fraud analysts do not resolve fraud disputes with your customers. You own the relationship, and you are best suited to resolve cases directly with your customer base. Therefore, no scripting or call monitoring is required.



Performance Results. Layering Managed Services with automated detection systems like Falcon has produced solid results for our large bank client. For each $1 invested in Managed Services, our bank clients realize a $30 average return. Our False Positive ratios continue to outperform the industry average. Consider that verification calls for suspicious card transactions have declined 24% for our large bank client meaning customers are not burdened with calls for legitimate transactions. Managed Services

saves money. We were able to improve fraud savings for a large US bank from $3 million to $21 million in just two years. Managed Services provides a money-saving layered approach to your fraud needs.

Conclusion

Fraud is ever present and will continue to be the bane of every financial institution whether big or small. Criminals continue to search for gaps in security or weak points in legacy based systems; financial institutions need to be just as vigilant in securing their enterprise. Point solutions are highly specific, and quite often these solutions are improperly sold as ERM systems. The truth is that many credit unions and banks wind up buying a dozen solutions from multiple vendors under the guise of real-time or cross-channel. But the reality is that these systems create disparate coverage that lacks a holistic view across the enterprise. Quatrro Processing Services has a highly effective and cost-conscious solution to meet your Enterprise Risk Management needs – from both automated tools to live transaction monitoring. And our layered approach closes the gap on fraud losses. Fraud is more than a threat to your profit margins. It is a threat to everything you've worked so hard to build – from customer loyalty to brand reputation. Staying ahead of fraud today takes a new generation of technology born from a commitment to both advanced systems and human intelligence. Quatrro Processing Services takes on the business of preventing fraud so you can concentrate on growing your business.

About Quatrro Processing Services

Quatrro is a global company consisting of 3,500 associates worldwide with a 21 year track record in Business Processing Services. Quatrro Processing Services is a U.S. division providing risk and fraud management, and card processing services. We offer an integrated suite of managed services and a highly-effective cross-channel fraud prevention platform called EnterpriseShield. Our fraud services cross the entire risk cycle spanning credit and debit cards, checks, ACH, wire, loans and more. By leveraging our Analytics and Transaction Monitoring solutions, your organization can more effectively manage your core competencies resulting in increased cost savings, streamlined operations and improved business processes.

For more information please visit: www.quatrroprocessing.com

To reach a sales associate please email: info@quatrroprocessing.com