July 2023

Consortium Data Sharing: A Valuable Tool in Fighting Fraud and Abuse

Jim Mortensen

This report is provided compliments of:

Early Warning®

July 2023

Consortium Data Sharing: A Valuable Tool in Fighting Fraud and Abuse

Jim Mortensen

Table of Contents

List of Figures

List of Tables

Summary and Key Findings

This report explores the benefits and considerations of using shared data to fight fraud while improving the customer experience. Commissioned by Early Warning® and based on interviews with fraud executives, this report begins with a market landscape of data-sharing consortia. It explores how banks and other financial institutions (FIs) can improve their fraud management capabilities and facilitate product usage by good customers through obtaining advanced insights into performance. The report then dives into a series of case studies that look at tangible use cases of FIs' use of Early Warning's consortium data. The key findings from this report follow:

- **Understanding current and historical performance is key to fraud prevention:** Knowing current and past behaviors of individuals, addresses, email addresses, accounts, transactions, devices, and other entities is an essential component of any risk management framework.
- **Shared databases come in a variety of forms: Credit reporting agencies (CRAs)** compile data and provide information and scores about individuals for evaluating the risk of account issuance and lending decisions, among other purposes, while **vendor-specific consortia** meet precise fraud and risk prevention purposes.
- **Consumer-permissioned data sharing has been on the rise:** Consumers can give access to their own data at FIs to link access to accounts for funds transfers or loan applications at other institutions. This has typically been achieved through data aggregators that leverage APIs that prompt the consumer to consent to third-party access to their data.
- **Fraud prevention can leverage shared data throughout the customer risk life cycle:** Shared data helps combat fraud, improve the customer experience, and facilitate transaction activity from the application process and managing and servicing to the approval of purchases, payments, and transfers.
- **Companies should address certain considerations concerning shared data usage:** Key considerations include the privacy and security of the data held, the governance structure over the provision and use of the data, and the regulatory framework that governs the data, including the rights of consumers.

Introduction

Data consortia exist within different frameworks and for a range of data types to aid in account origination, ongoing authentication, and life cycle risk assessment. These consortia provide FIs and merchants with fuel to properly assess the risk of consumer transactions and the extension of additional products and account privileges. To effectively benefit from data-sharing opportunities, users should understand the associated consumer obligations, regulatory requirements, and data integrity provisions that apply to both the provision of data to sharing consortia and the use of that data in making fraud risk decisions.

This Impact Report will provide a view into the consortium data-sharing market landscape and explore the key benefits and challenges of leveraging consortium data sharing for detecting and preventing fraud. In addition, the report will discuss the existing frameworks under which data is leveraged for fraud prevention use cases and present a specific case study of the National Shared Database^{SM} Resource maintained by Early Warning.

Methodology

This Impact Report was informed by Datos Insights' ongoing industry research on fraud trends, which includes quantitative and qualitative studies of financial services firms, vendors, and consumers. It is further augmented by interviews with solution providers about topics that are top of mind to prospective buyers and direct conversations with fraud and security professionals fighting to protect their financial services firms. To inform the case studies, Datos Insights interviewed multiple Early Warning bank clients of varying asset sizes about their experience leveraging consortium-driven fraud solutions.

The Consortium Data-Sharing Market Landscape

Consortium data sharing exists in a variety of forms and can address a wide range of specific risk issues. These consortia are used to report and detect fraud in addition to their use for credit purposes. Built from multiple data sources, consortia approaches can help establish holistic and accurate profiles of the behaviors and the historical performance of individuals, devices, addresses, and other entities. These are critical fuel to propel fraud detection engines.

Data is shared in various ways through consortia and directly by third parties. The data types shared also vary by the breadth of the information, contribution and sharing methods, and purposes for which the data is used. Table A summarizes these data-sharing conduits.

Table A: Data-Sharing Conduits

Mechanism	Description
CRAs	These organizations compile data and provide customer information and associated risk scores to support the evaluation of the risk of account issuance and lending decisions, among other purposes. CRAs can be broadly split into two categories: • **National CRAs:** Large credit bureaus compile information their users provide containing credit tradelines and other data for making new risk decisions. • **Specialty CRAs:** These companies collect and share information about accounts, employment history, and other noncredit accounts and purposes.
Vendor-specific consortia	These shared data sources exist to meet specific fraud prevention purposes and use cases. They typically support a specific vendor's risk product(s) by sharing data across that vendor's customer base to improve fraud detection.
Consumer-permissioned	Consumer-permissioned data includes transactional and account attribute data, such as the name on the account, current balance, and tenure. The data is typically from an FI, such as a bank or brokerage firm, where the consumer provides permission to access their data.

Source: Datos Insights

CRAs

As previously described, CRAs can be split into two broad categories: national CRAs and specialty CRAs (Table B). Both types of CRAs address a range of use cases and are private companies regulated under the Fair Credit Reporting Act (FCRA), which governs the collection and disclosure of consumer information.

Table B: CRA Landscape

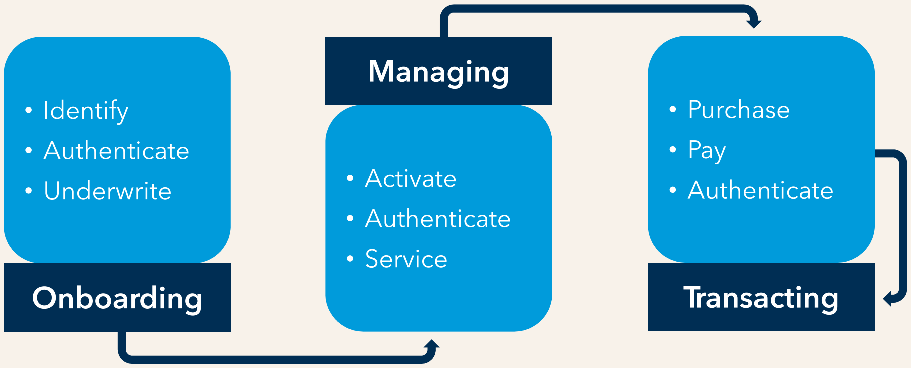
Primary CRA type	Financial use cases	Fraud types	Select companies
National	• Lending account applications • Lending account monitoring • Rental applications • Telecomm applications • Utility applications	• Identity theft • Synthetic identity • First-party fraud • Internal fraud	• Experian • Equifax • TransUnion
Specialty	• Deposit account applications • Deposit account monitoring • Extended lending underwriting • Mortgage applications • Payments	• Identity theft • Synthetic identity • Deposit fraud • Payment fraud • Internal fraud	• Certegy Payment Solutions • FIS • CrossCheck • Early Warning • Global Payments • Fiserv • CoreLogic Credco • Innovis • LexisNexis Risk Solutions • National Consumer Telecom & Utilities Exchange

Source: Consumer Financial Protection Bureau (CFPB)

Shared Data Advantages in the Fight Against Fraud

Regardless of the source of the shared data, consortium intelligence can be applied to several use cases throughout the customer life cycle. From streamlining the application process to managing and servicing to approving purchases, payments, and transfers, shared data can help combat fraud, improve the customer experience, and facilitate transaction activity (Figure 1).

Figure 1: Customer Life Cycle



Source: Datos Insights

Onboarding

The application and onboarding process is the most important point in the customer life cycle. It is the first chance to start the relationship on a positive note—an opportunity to create a great first impression. Unfortunately, it is also the point when the least is known about the customer, their behaviors and preferences, their potential profitability, and perhaps most importantly, their level of risk. Shared intelligence helps to advance the level of knowledge from a risk perspective, inform and expedite the approval decision, and mitigate the friction that needs to be applied to positively identify the customer.

Managing

Managing and servicing accounts requires continual authentication within each channel the customer uses. Online servicing can be the most vulnerable channel, as it provides a cloak of anonymity compared to branch interactions. Hence, having the tools and intelligence to know who is on the other end becomes critical. While companies have leveraged device intelligence and behavioral biometrics tools as signals to support customer authentication, the power of these capabilities is multiplied when their intelligence is fueled by shared data.

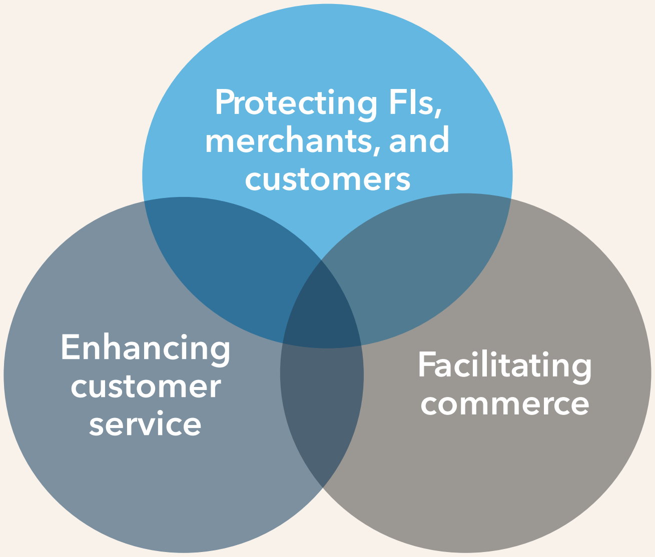
Transacting

Transactional moments of truth are crucial to merchants and FIs alike. The core reason that consumers use credit cards and DDAs is to pay for goods and services they want or need. If consumers experience needless, unreasonable, or excessive friction when trying to make payments or purchase goods online, it undermines the reason they have the account. Leveraging a network of intelligence can ensure that those key moments of truth are managed well and friction is applied only where required.

Benefits of Shared Data in Fraud Prevention

Data sharing through consortia yields numerous interrelated benefits. Chief among them are protecting FIs, merchants, and consumers; improving the customer experience; and facilitating commerce (Figure 2).

Figure 2: Benefits of Shared Data Through Consortia


Protecting FIs, merchants, and customers
Enhancing customer service
Facilitating commerce

Source: Datos Insights

Protecting FIs, Merchants, and Customers

Sharing data for fraud prevention benefits all parties to the transaction except the fraudster, as all parties pay for the cost of fraud:

- The FI and merchants bear the immediate cost in the form of fraud losses and operational expenses associated with preventing and mitigating fraud, and protecting the enterprise and its customers. The expense of building and sustaining robust fraud systems and the underlying infrastructure can be significant.
- Most FIs and merchants will account for the cost of fraud into their margins to maintain profitability, so higher fraud typically means higher prices for financial services and e-commerce. Also, when fraud occurs on their accounts or identities, consumers bear some burden in the remediation process, often being inconvenienced in resolving the issue.

Improving the Customer Experience

A key benefit within business cases that attempt to justify new fraud prevention capabilities is how they improve the customer experience. Fraud loss prevention and operational expense reduction are often viewed as the primary drivers, but improving the customer experience is another vital consideration, as it can support increased customer loyalty and overall revenue.

Facilitating Commerce

The availability of shared data sources that help prevent fraud has a broad impact on society regarding the facilitation of commerce. Increasing the visibility into the risk of individuals, devices, emails, phones, and other entities elevates the confidence of providers of goods and services in conducting business profitably. This transparency, in turn, supports market efficiency and stability in two crucial ways. First, financial service providers and merchants can draw on these data sources to evaluate prospects and transactions more effectively. Secondly, regulators expect FIs to support the financial system’s stability by appropriately vetting their customers and managing the risk within their portfolios.

Early Warning—A Leader in Consortium Data

Early Warning Services LLC is owned by seven of the nation's largest banks and has been a long-standing data and technology provider and protector of the financial system serving a network of approximately 3,500 FIs, government entities, and payment companies. Today, Early Warning is best known as the owner and operator of the Zelle Network®. Early Warning solutions enable real-time funds availability for a variety of payment types through its financial services network. The company also assists FIs, retail merchants, payment processors, and other financial entities in detecting and preventing fraud associated with bank accounts and payment transactions.

As a specialty CRA, Early Warning was created in the 1990s out of a need by FIs to understand the status of DDAs at other institutions to determine funds availability on deposited items. Early Warning's initial service consisted of shared data between institutions, including the contribution of the required data and responses to inquiries on items presented for deposit. From these responses, FIs could determine whether to place an extended hold on an item or provide immediate funds availability.

Early Warning's National Shared Database Resource

Early Warning's National Shared Database℠ Resource holds and manages the data that fuels the company's fraud and risk solutions. The data is leveraged to power its solutions across various technology platforms.

Contributed Data Sets

The data sets populated within the National Shared Database Resource are provided by contributor institutions on a give-to-get basis concerning the products and services each institution uses. In general, subject to certain restrictions, the data can also be used in any of the products, or capability bundles, permitted by the National Shared Database Operating Rules, regardless of whether or not that contributor uses that specific capability.

Governance and Data Integrity

The National Shared Database Resource is governed by a set of operating rules that Early Warning maintains. Its data integrity program is designed to ensure that contributed data sets adhere to the operating rules and technical specifications. This program includes multiple layers of monitoring and data integrity controls that are regularly tested to ensure adherence to the operating rules and technical specifications.

Solution Operation and Fraud Prevention Value

The data aggregated within the National Shared Database Resource enriches risk intelligence within the Early Warning product suite. The company's capability bundles are fueled by a combination of data sets most relevant to the specific risk decision. The solutions operate on an inquiry-and-response response basis. Each user inquiry sent to a respective service receives a response that can be used by the inquirer to inform the relevant risk decision on the application or transaction.

Early Warning, Client Success Stories

The Early Warning National Shared Database Resource powers the fraud prevention and mitigation capabilities within the company's solutions throughout the customer life cycle. FIs of all sizes get value from the visibility provided by sharing data at key risk decision points. The following three success stories from banks of different sizes illustrate the uses of consortium data through Early Warning.

Regional Bank (US$50 billion to US$100 Billion in Assets)

A regional bank concentrated in the southeastern U.S. needed to manage the risk of items and determine funds availability for their customers on a real-time basis when deposits were made at a branch. The bank offers consumers deposit, commercial banking, and wealth management services.

The bank also needed to validate the ownership of accounts at other banks used to fund new accounts. Ownership validation was particularly important because the new accounts were being funded and drained before the sending bank victim noticed the transfer. More recently, the bank noted that home equity lines of credit were being paid down with the account of others, and the line of credit was being run up again before the fraudulent payment was discovered, a fraud technique known as a bust-out.

The Solution Set: Early Warning's Verify Deposit and Verify Payment

The bank realized it needed a way to quickly determine the status of the accounts that items were drawn on and validate the ownership of off-us accounts. Considering time is of the essence concerning online transfers, the speed of the account ownership validation process became crucial; trial deposits were not working, given the time frames involved.

To address these challenges, the bank implemented Early Warning's Verify Deposit real-time solution (formerly Real-Time Deposit Chek®) and Verify Payment (formerly Real-Time Payment Chek® with Account Owner Authentication). With the implementation, the bank could leverage the capability bundles powered by the National Shared Database Resource to place extended holds and validate ownership online and at the branch to address the fraudulent payments made on home equity lines of credit. The bank also leveraged a data aggregator to provide coverage for accounts not in the Early Warning financial services network as a second option within the Waterfall. However, the Early Warning solution provides a better, more secure customer experience because it does not require customers to expose their online login credentials for other institutions.

Table C provides high-level example results for similarly situated FIs using the Verify Deposit solution. The results include total inquiries sent to the service, the volume and value of high-risk alerts delivered to the institution, and the potential fraud loss avoidance benefit of these institutions.

Table C: Verify Deposit, High-Level Example Results, Regional Banks

Metric	Result
Total inquiries	5 million
High-risk alert volume	16,000
High-risk alert value	US$42 million
Potential fraud loss avoidance	US$4 million

Source: Early Warning Services LLC

Large Regional Bank (US$200 Billion to US$300 Billion in Assets)

A large regional bank serving customers in several eastern U.S. states wanted to ensure that it had a broader view of customer behaviors to evaluate risk, make decisions, and orchestrate actions more effectively. The bank already used the batch versions of Verify Identity (formerly Identity Chek® Service) to screen applications for new accounts, Verify Deposit to evaluate deposited items, and Verify Payment to risk-assess payments. The bank provides checking, savings, certificate of deposit, and credit card products to consumers and businesses in addition to insurance and investment solutions.

The bank also wanted to create a more uniform customer experience across all channels. Having consistent information available for risk decisioning so that relevant information is considered was critical to inform the risk decisions, and actions, taken on transactions. Ensuring consistency of all risk decisioning would be equally important from a regulatory perspective.

The Solution: Early Warning's Verify Deposit With Verify Account

The bank was already successfully using batch solutions, so it decided to implement the real-time versions to ensure that its transaction decisioning incorporated the most up-to-date information available. With the real-time versions, the bank could also leverage Verify Account (formerly Account Owner Authentication) to validate ownership, moving away from antiquated trial deposits and addressing unauthorized ACH fraud issues.

The bank could load the history of data received from Early Warning within the bank's orchestration platform and build the appropriate context to obtain a more comprehensive view of customer activity and risk profiles. Each transaction is evaluated based on the information on the account at that time, but the context provided by the historical data informs the decision-making, the disposition, and the related course of action. This supported greater consistency across the customer experience.

Table D provides high-level example results for similarly situated FIs using the Verify Deposit solution. The results include total inquiries sent to the service, the volume and value of high-risk alerts delivered to the institution, and the potential fraud loss avoidance benefit of these institutions.

Table D: Verify Deposit, Fraud Prevention Opportunity, Large Regional Banks

Metric	Result
Total inquiries	10 million
High-risk alert volume	28,000
High-risk alert value	US$126 million
Potential fraud loss avoidance	US$10 million

Source: Early Warning Services LLC

National Bank (Over US$300 Billion In Assets)

A top national bank serving customers throughout the U.S. desired to move to a new account risk score that focused on the specific behavior of first-party fraud, which was the costliest in terms of fraud losses. The bank was using another risk solution for screening new account applications that leveraged data sources inconsistent with the bank's policies, making it important to move to a new capability.

With locations in major cities such as Atlanta, New York, Boston, and San Francisco, the bank expanded its digital model to provide products and services to its customers nationally. Given the bank's investment in the online channel for new account issuance, it needed an effective, efficient, and fully compliant tool to address losses. The bank sought a real-time solution that could provide insights into future performance that it was not getting from its current provider.

The Solution: Early Warning's Predict New Account Risk

The bank implemented Early Warning's Predict New Account Risk solution (formerly New Account Scores), which predicts potential first-party fraud at the time of application. This solution leverages Early Warning's Shared Fraud database and other data contributed to the National Shared Database, such as account status and related check, ACH, and return items on applicant-owned accounts. The returned risk score and summarized attributes correlate to a likelihood of first-party fraud occurring on the account over the next nine months, enabling the bank to specify the level of risk it is willing to take on new accounts.

The bank found that it outperformed its prior vendor solution. The Early Warning risk score had greater coverage, allowing the bank to understand the risk of a greater number of applicants. The bank was able to identify and stop more fraud while lowering false positive rates and elevating the quality of declines in terms of the ability to explain the rationale for their decision to the applicant. This has a favorable impact on the size and profitability of a bank's portfolio of DDAs.

Table E provides high-level example results for similarly situated FIs using the Predict New Account Risk—First-Party Fraud score. The results include total inquiries sent to the service, the volume of high-risk alerts and related potential fraud loss avoided, and the false positive ratio typically experienced.

Table E: Predict New Account Risk—First-Party Fraud, Fraud Prevention Opportunity, National Banks

Metric	Result
Total inquiries	2 million
Fraud alert volume	39,000
Potential fraud loss avoidance	US$39 million

Source: Early Warning Services LLC

Conclusion

Managing fraud and abuse in today's increasingly complex environment is fraught with challenges, from an array of evolving threat vectors to the range of ways in which customers interact with their FIs. Fraud prevention professionals must employ every tool available to effectively mitigate losses without adversely impacting business growth or disrupting the customer experience. The ability to balance these objectives is enhanced by data-sharing consortia that provide increased visibility and intelligence of risky entities. FIs and their fraud prevention leaders should consider the following in pursuing and unlocking the power within data-sharing consortia:

- **Understand the data consortia market landscape and different sharing approaches:** Ensure you are aware of the available data within the various consortia that may be relevant to your lines of business and the related coverage.
- **Review the organizational data needs at each point throughout the customer risk life cycle:** Continually examine your enterprise risk processes and the touch points across the control framework in which consortium data could provide value.
- **Align the available data-sharing options to fraud prevention needs:** With a strong understanding of the market landscape and risk process data needs, determine how best to meet your requirements with the available consortia data sources.
- **Understand regulatory, security, and privacy issues:** It is critical to consider a consortia's data privacy and security regime, the governance structure, and the regulatory framework that governs data sharing.
- **Monitor contributions of data to consortia and understand all uses:** Since most data consortia require that like data be furnished to the consortia in exchange for access, ensure that the consortium has established an effective monitoring and control framework that promotes data integrity.
- **Maintain awareness of data-sharing options as the market evolves: As** new data sources and providers emerge, keep abreast of the market, particularly with respect to vendor-specific data as new providers frequently emerge.

About Datos Insights

Datos Insights is an advisory firm providing mission-critical insights on technology, regulations, strategy, and operations to hundreds of banks, insurers, payments providers, and investment firms—as well as the technology and service providers that support them. Comprising former senior technology, strategy, and operations executives as well as experienced researchers and consultants, our experts provide actionable advice to our client base, leveraging deep insights developed via our extensive network of clients and other industry contacts.

Contact

Research, consulting, and events:

sales@datos-insights.com

Press inquiries:

pr@datos-insights.com

All other inquiries:

info@datos-insights.com

Global headquarters:

6 Liberty Square #2779
Boston, MA 02109
www.datos-insights.com

Author information

Jim Mortensen

jmortensen@datos-insights.com