IBM Analytics
Solution brief

Financial

IBM Algo FIRST for insurance

Qualitative and quantitative database of external risk loss events

Highlights

- Helps users understand, identify and manage operational risk
- Recognized by analysts and practitioners alike for its industry-leading coverage
- Provides thousands of real-life case studies based on external risk loss events.
- Part of the IBM Algo Risk Content on Cloud family of products

IBM® Algo FIRST® highlights operational risk events, control breakdowns and management responses to help insurance providers prevent losses before they occur. Subscribers can proactively apply lessons learned from almost 15,000 real-life case studies to help minimize their risk exposure and enhance internal controls.

Recent additions encompass several events related to insurance, including contingent commission payments, annuity-related sales practices, finite reinsurance, vanishing premiums, mortgage endowments, regulatory violations and European Union anti-competition fines.

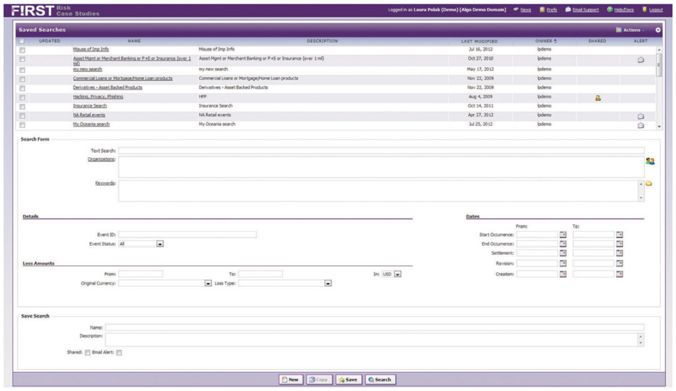
One of the industry's most respected external risk loss databases

Insurance companies are complex entities that are ultimately responsible for managing the financial future of others. As a result, they are at risk of losing their franchise if they are unable to preserve their good name.

A worst possible scenario for an insurance company is one where it finds itself the target of lawsuits, or the subject of high-profile news stories linked to mis-selling, breach of fiduciary trust, breach of contract, or an inability to meet its obligations. History has shown that the failure to understand and manage these potential risks can lead to a catastrophic loss in franchise value.

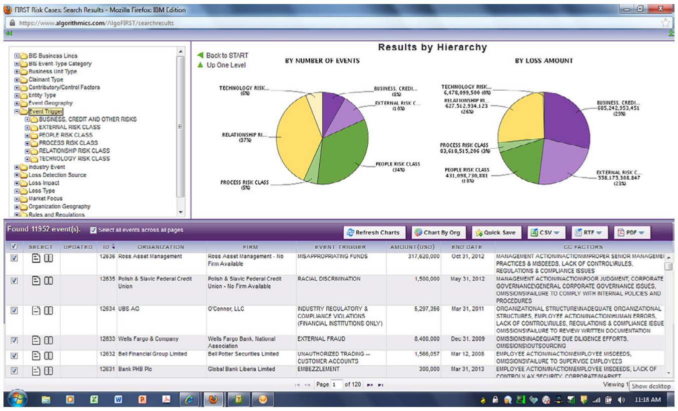
One important strategy for proactively managing risk is to learn from the experience of others. The Algo FIRST database contains distinct, real-life case studies that provide the buy-side community with qualitative and quantitative analysis of large loss events. This content, which includes insight into key triggers, contributory factors, management responses, and associated control breakdowns, can help insurance providers prevent similar mishaps in their own firms.

One of the industry's only research tools that puts real-life case studies within an operational risk framework, Algo FIRST is an ideal supplement to internal data for self-assessment and scenario modeling. Charts and graphs, free-text search, in-depth case studies, and essential content for self-assessment programs help make Algo FIRST an invaluable resource for insurance providers. Designed to be available on a subscription basis, the Algo FIRST database is accessed through the internet and does not require installed software.



□	UPDATED	NAME	DESCRIPTION	LAST MODIFIED	OWNER	SHARED	ALERT
□		Misuse of Imp Info	Misuse of Imp Info	Jul 16, 2012	lpdemo		
□		Asset Mgmt or Merchant Banking or P+S or Insurance (over 1 mil)	Asset Mgmt or Merchant Banking or P+S or Insurance (over 1 mil)	Oct 27, 2010	lpdemo		
□		my new search	my new search	May 17, 2012	lpdemo		
□		Commercial Loans or Mortgage/Home Loan products	Commercial Loans or Mortgage/Home Loan products	Nov 22, 2009	lpdemo		
□		Derivatives - Asset Backed Products	Derivatives - Asset Backed Products	Nov 22, 2009	lpdemo		
□		Hacking, Privacy, Phishing	HPP	Aug 4, 2009	lpdemo		
□		Insurance Search	Insurance Search	Oct 14, 2011	lpdemo		
□		NA Retail events	NA Retail events	Apr 27, 2012	lpdemo		
□		My Oceania search	My Oceania search	Jul 25, 2012	lpdemo		

Figure 1: Screen capture of the Algo FIRST home page



☑	SELECT	UPDATED	ID	ORGANIZATION	FIRM	EVENT TRIGGER	AMOUNT(USD)	END DATE	CC FACTORS
☑			12636	Ross Asset Management	Ross Asset Management - No Firm Available	MISAPPROPRIATING FUNDS	317,620,000	Oct 31, 2012	MANAGEMENT ACTION/INACTION\IMPROPER SENIOR MANAGEMEI PRACTICES & MISDEEDS, LACK OF CONTROL\RULES, REGULATIONS & COMPLIANCE ISSUES
☑			12635	Polish & Slavic Federal Credit Union	Polish & Slavic Federal Credit Union - No Firm Available	RACIAL DISCRIMINATION	1,500,000	May 31, 2012	MANAGEMENT ACTION/INACTION\POOR JUDGMENT, CORPORATE GOVERNANCE\GENERAL CORPORATE GOVERNANCE ISSUES, OMISSIONS\FAILURE TO COMPLY WITH INTERNAL POLICIES AND PROCEDURES
☑			12634	UBS AG	O'Connor, LLC	INDUSTRY REGULATORY & COMPLIANCE VIOLATIONS (FINANCIAL INSTITUTIONS ONLY)	5,297,356	Mar 31, 2011	ORGANIZATIONAL STRUCTURE\INADEQUATE ORGANIZATIONAL STRUCTURES, EMPLOYEE ACTION/INACTION\HUMAN ERRORS, LACK OF CONTROL\RULES, REGULATIONS & COMPLIANCE ISSUE OMISSIONS\FAILURE TO REVIEW WRITTEN DOCUMENTATION
☑			12633	Wells Fargo & Company	Wells Fargo Bank, National Association	EXTERNAL FRAUD	8,400,000	Dec 31, 2009	OMISSIONS\INADEQUATE DUE DILIGENCE EFFORTS, OMISSIONS\OUTSOURCING
☑			12632	Bell Financial Group Limited	Bell Potter Securities Limited	UNAUTHORIZED TRADING -- CUSTOMER ACCOUNTS	1,566,057	Mar 12, 2008	EMPLOYEE ACTION/INACTION\EMPLOYEE MISDEEDS, OMISSIONS\FAILURE TO SUPERVISE EMPLOYEES
☑			12631	Bank PHB Plc	Global Bank Liberia Limited	EMBEZZLEMENT	300,000	Mar 31, 2013	EMPLOYEE ACTION/INACTION\EMPLOYEE MISDEEDS, LACK OF CONTROL\LAX SECURITY, CORPORATE/MARKET

Figure 2: Screen capture of Algo FIRST query results

Algo FIRST database sample case study

Premera Blue Cross (excerpt from Event #14261)

Data security is a pressing concern across all sectors of the financial services industry. Premera Blue Cross, a Washington state-based health insurance provider disclosed on March 17, 2015, that confidential data of up to 11 million current and former customers had been compromised. The insurer discovered the systems breach on January 29, 2015, but it believes that the perpetrators may have first gained unauthorized access as early as May 5, 2014.

The stolen information included names, birthdays, e-mail and physical addresses, telephone numbers, Social Security numbers, and bank accounts. In addition, the perpetrators also accessed sensitive medical data including insurance claims and clinical information. Insurance regulators in at least three states—Washington, Oregon, and Alaska—launched probes into the incident, which was also investigated by the Federal Bureau of Investigation (FBI).

According to Premera Blue Cross, which primarily serves customers in the northwestern United States, the breach affected approximately 11 million current and former customers, as well Blue Cross and Blue Shield policyholders from other US states who might have obtained medical treatment while in the states of Washington or Alaska. Those affected did business with Premera at some point after 2002.

Neither Premera nor FBI officials would discuss in detail how the attack was executed. Some security observers including the Wall Street Journal suspected that—as with a breach of Anthem, another-health insurance provider, (see Event #14138)—hackers based in China or associated with the Chinese government might have been involved.

In part, this is due to Premera's decision to hire the same consulting firm to conduct a forensic investigation into the attack and to re-secure the insurer's network. Well-known security researcher Brian Krebs noted that the firm "specializes in tracking and blocking attacks from state-sponsored hacking groups, particularly those based in China."

The Wall Street Journal also reported suspicions that the Premera breach, like the one at Anthem, had "links to China based on the hacking software used." The sources noted that the digital signatures used in the malware used to target Anthem's network were similar to malware targeting Premera.

Lax security was among the contributory factors to the data breach. Federal regulators had warned Premara about ten specific vulnerabilities that they had discovered in the company's system. They included a failure to patch vulnerabilities in timely manner; use of software that was known to have security problems and was so old that it was no longer supported; and use of unsecured server configurations.

In April 2014—three weeks before the breach is believed to have begun—the U.S. Office of Personnel Management (OPM) told Premera that its audit of the insurer had found ten weaknesses in its network security procedures. The insurer did not respond to OPM's findings until June 30, 2014, when it purportedly pledged to fix the alleged deficiencies before the end of 2014. While it is unclear whether the perpetrators used any of the vulnerabilities found by federal regulators, the slow response to the report suggests a lack of urgency with regard to network security issues.

As part of its corrective actions to address the breach, the insurer promptly notified the FBI and retained Mandiant to conduct a forensic investigation into the breach and to ensure that its network was secure and free of malware.

Management also responded by issuing an apology to those affected by the breach, noting that it had seen no evidence that the compromised information had been used illicitly. Premera said it would send letters to individuals who might have had their personal information compromised, and would offer two years of free credit-report monitoring and identity-theft protection.

Premera had said that it waited to inform the public based "on strong advice that we should block the attack and cleanse our IT systems before the announcement. We were warned that other organizations affected by such incidents that ignored this advice experienced the attackers engaging in even more malicious activity. That means affected individuals would have been at greater risk had Premera announced before finishing its investigation and enhancing its IT security."

At least five civil lawsuits, all filed in U.S. District Court for the Western District of Washington, have been brought by individuals seeking class-action status and alleging damages incurred as a result of this breach. All were pending as of March 30, 2015.

The Premera breach compounded concerns regarding security at insurance companies operating in the healthcare industry. A complete set of stolen health insurance credentials can reportedly sell on the black market for as much as USD 20 each, a far higher sum than the dollar or two it costs to purchase a stolen U.S. credit card number with its associated security codes. A healthcare record includes a far greater range of personal information that cyberthieves can use in a number of ways, including phishing attacks and direct identity theft.

Criminals can also use some types of medical information, for instance evidence that an individual has been treated for substance abuse or a sexually transmitted disease, for blackmail purposes. "What we've seen in the last few years is that attackers have realized the economics of healthcare data are very, very attractive," said Lee Weiner, Senior Vice President at Rapid7, a cybersecurity firm.

The insurance industry is also at risk to fraudulent claims. Pam Dixon, executive director of the World Privacy Forum, noted that stolen healthcare data can be far more dangerous to individuals than stolen financial information. Stolen healthcare information can be used to commit insurance fraud, for instance, and this can affect a victim's ability to obtain prescription drugs and medical treatments in a timely manner.

Key benefits and features

Provides a better understanding of potential exposures

Algo FIRST case studies can be shared among departments, providing valuable content for use in management reports, committee or board presentations or discussions, internal newsletters, self-assessment workshops, and scenario-based models. Charts and graphs allow quicker understanding of loss breakdowns, while the internet-based subscription helps ensure that users across the organization can more quickly access Algo FIRST without additional infrastructure cost.

Helps minimize risk exposure

By proactively applying lessons learned, insurance companies can improve internal controls, reduce investment risk, and create better understanding of new product research processes before potential losses or exposures occur.

Enhances trend analysis

Firms gain the ability to examine commonalities among a series of events and to track emerging patterns. By benchmarking internal loss history against the event experience of peers, organizations can use Algo FIRST to help improve their competitive insights.

Helps reduce investment risk

Insurers improve new product research processes by identifying potential risk exposure by product type, so the appropriate control measures can be put in place. Management can also reference Fitch ratings or Scaling data for banks and insurers, which is linked to the timing of events, to see if there are contextual references of how events might have impacted the cost of capital.

Increases access to relevant insights

IBM operational risk research analysts have a background in financial analysis. This experience helps ensure that they understand which loss event details are relevant to insurance companies and that these insights are passed along to subscribers.

Allows for easier data export

Users can create customized searches and then download information in CSV, RTF or PDF formats for use in other internal documents or knowledge-based systems. For those who want to integrate FIRST into systems by using automation or filtering routines, Algo FIRST is available in three data add-on formats:

- An XML version that you can use to incorporate Algo FIRST data through direct feed into internal or external operational risk, compliance, enterprise risk or other knowledge-based systems
- A FastMap version that you can use to incorporate Algo FIRST data through direct feed into the IBM OpenPages® Operational Risk Management module
- A Services Directory Integrator (SDI) version that you can use to incorporate Algo FIRST data using the SDI ETL tool into the IBM OpenPages Operational Risk Management module

In-depth case studies

Loss events are detailed with analyses of key factors, including control breakdowns, regulatory rule violation information, management responses to events, graphs and charts, and industry lessons learned. Special coverage is provided for catastrophic (tail) events, which are detailed with timelines to allow for day-by-day or hour-by-hour analysis of breakdowns that led to loss.

Extensive search functions

Free-text and hierarchical searches allow for user identification of events by natural language or keyword node terms. The powerful search engine of Algo FIRST enables users to combine search concepts or search by several factors, including product type, geography, loss type, event trigger and control breakdowns. Basel II categorizations and Boolean search are also supported in the advanced search function of Algo FIRST. Users can create customized searches, save them, and then be notified by email when new events or updates are available.

Access to online newsletter

Algo FIRST Database subscribers also receive a monthly newsletter. This monthly online publication is designed to raise awareness of topical issues that can impact daily business operations. This newsletter also provides excerpts from relevant case studies to highlight how Algo FIRST informs your risk program.

About IBM Analytics

IBM Analytics software delivers data-driven insights that help organizations work smarter and outperform their peers. This comprehensive portfolio includes solutions for business intelligence, predictive analytics and decision management, performance management, and risk management.

Analytics solutions enable companies to identify and visualize trends and patterns in areas such as customer analytics, which can have a profound effect on business performance. They can compare scenarios, anticipate potential threats and opportunities, better plan, budget and forecast resources, balance risks against expected returns and work to meet regulatory requirements. By making analytics widely available, organizations can align tactical and strategic decision-making to achieve business goals. For further information, visit **ibm**.com/analytics.

Request a call

To request a call or to ask a question, visit **ibm.com**/analytics/us/en/contact-us. An IBM representative will respond to your inquiry within two business days.

Notice

The information contained in this documentation is provided for informational purposes only. Although efforts were made to verify the completeness and accuracy of the information contained in this document, it is provided “as-is” without warranty of any kind, Express or Implied. In addition, this information is based on the IBM Algorithmics® current product plans and strategy, which are subject to change by Algorithmics without notice.

Algorithmics will not be responsible for any damages arising out of the use of, or otherwise related to, this document or any other materials. Nothing contained in this document is intended to, or shall have the effect of creating any warranty or representation from Algorithmics (or its affiliates or their suppliers and/or licensors); or altering the terms and conditions of the applicable license agreement governing the use of Algorithmics software. References in this publication to Algorithmics products or services do not imply that Algorithmics intends to make them available in all countries in which Algorithmics operates.

For any reference to an Algorithmics software program, the software program can be used to help the customer meet compliance obligations, which may be based on laws, regulations, standards or practices. Any directions, suggested usage, or guidance provided by the software program, or any related materials, does not constitute legal, accounting, or other professional advice, and the customer is cautioned to obtain its own legal or other expert counsel. The customer is solely responsible for ensuring that the customer and the customer’s activities, applications and systems comply with all applicable laws, regulations, standards and practices. Use of the software program, or any related materials, does not guarantee compliance with any law, regulation, standard or practice.

Any information regarding potential future products and/or services is intended to outline Algorithmics’ general product and service direction and it should not be relied on in making a purchasing decision. Any information mentioned regarding potential future products and services is not a commitment, promise, or legal obligation to deliver any material, code, functionality or service. Any information about potential future products and services may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for Algorithmics’ products or services remains at Algorithmics’ sole discretion.

© Copyright IBM Corporation 2016

IBM Corporation
Route 100
Somers, NY 10589

Produced in the United States of America
December 2016

IBM, the IBM logo, ibm.com, Algo, Algo FIRST, Algorithmics and OpenPages are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Please Recycle