accenture

Strategy | Consulting | Digital | Technology | Operations

Fighting Financial Crime With Data

High performance. Delivered.

Introduction

The "digitization" of global commerce has given consumers greater choice, greater convenience and lower prices. The use of digital and mobile devices to access bank services and make payments, in particular, is growing rapidly.

This digital revolution, however, has also created enormous opportunities for the perpetrators of fraud and financial crime, with estimates of losses to cyber-crime ranging from a few hundred million up to a trillion dollars.[1] While estimates vary, it is clear that security and data breaches result in multi-million dollar losses. The findings of a 2013 Ponemon research indicated that the average financial impact to companies for each incident was $9.4 million, with respondents estimating that the average potential financial risk of future incidents is $163 million.[2]

The increasingly sophisticated techniques used by cyber criminals — including undetected malware and unauthorized access to mobile devices and sensitive data — have led financial services organizations to pursue new approaches to preventing and detecting such activities.

Financial services organizations must also deal with a host of new regulatory initiatives. Regulators such as the Bank of England rate cyber-attacks as the biggest threat to the banking system.[3]

Most cyber-attacks involve the loss of confidential information. As new products are introduced, with new channels for distribution, new vulnerabilities arise, and banks must develop new techniques to address them.

The challenge for banks and other financial services organizations is considerable. They must be able to demonstrate to consumers that they have adequate safeguards in place to protect confidential information (and, ultimately, consumers' assets). They must also be able to demonstrate to regulators that they have active programs in place to prevent financial crime, with controls that are robustly enforced and standardized across business units and geographies.

Finally, banks need to demonstrate to shareholders that they can manage the monetary and financial risks from financial crime. More than half of financial services firms have said that spending on financial crime prevention and reputation management has increased by over 20 percent in recent years, at a time when there is a sharp focus on cost management in every sector of the business.[4]


ANALYTICS
FRAUD
CYBER-ATTACKS

The Data Dilemma

The management and monitoring of vast quantities of data is one of the central challenges for banks in their efforts to battle cyber-crime. Banks feed data from a diverse set of sources into centralized monitoring systems. Global banks obtain customer and transaction data from various systems, and maintaining the quality of data in terms of accuracy, timeliness and other factors can be quite difficult.

These difficulties can be compounded by the lack of clear demarcation of roles and responsibilities among the businesses, the IT function, and the fraud and financial crime units. An even bigger problem is the failure to align data strategy with the overall organizational strategy.

Ultimately, banks need a more integrated view of relevant data. To accomplish this, they will have to pool data that, in many cases, has been stored and processed independently by division, channel or geography. Although data integration is likely to be more effective when there is a central repository of customers – along with centralized systems – this is not the case in many organizations. Accenture's research shows that just over half of financial services organizations have a single view of their customers, and only about half have a single system to comply with anti-money laundering (AML) directives.[5] Only about 60 percent have a single system for sanctions screening.[6] Fraud management data, as well, is typically fragmented across layers of channel and product-based controls.

An Integrated Approach Using Data and Analytics

Given the large and increasing volumes of transactions and accounts to be monitored, it is often difficult – even for seasoned investigators – to handle the volume of transactions using traditional, linear data views. New technologies and solutions, however, can make it easier for banks, not only to create an integrated data set, but to bring sophisticated analytics to bear on the data, generating useful insights to help prevent and detect financial crime. There are three major elements needed to make this happen:

1. Enhancing the Quality of Data

The quality of insights derived from any analysis will be highly dependent on the quality of data provided. Financial services firms use a variety of internal and external data sources to fight crime, but many firms – particularly universal banks operating in different regions and across different lines of business, using multiple systems and data sources – face data quality issues.

The first step in improving data quality is to define the right data quality metrics. This requires a comprehensive set of metrics to measure and improve data quality on an ongoing basis. These metrics should address, among other aspects, the data's accuracy and integrity; its completeness (the availability of complete data for transaction screening including customer information, transaction amounts and other data points); and its timely availability, to support real-time analytics.

The second step is to establish central data screening and reconciliation. Global banks are driving enterprise-level data quality improvement initiatives. Customer account data and transactional data used by different AML and fraud management systems are collected from various sources. Screening and cleaning the data enhances the quality of the analysis and helps reduce the number of false positives, which take considerable time and effort to address.

The third step is to improve data governance. Most leading organizations now have a Chief Data Officer (CDO). In order to improve the way data is used, however, it is essential to establish clear lines of responsibility among the business process owners, their technology counterparts and the fraud and financial crime management teams. This requires strong data governance with well-delineated rules for data ownership and data quality. The focus of quality improvement should be on those data elements such as risk classification that drive key decisions and are featured in major reports.

2. Analytics to Transform Data into Information and Information into Insight

For most organizations, a lack of data is not the problem. The real problem is a lack of the right data. Banks typically have greater access to centralized data than they have ever had, but most banks use less than five percent of the available data in making decisions related to financial crime prevention;[7] much of the rest of the data is considered too expensive to deal with.

There is a widening gap between companies who understand that data is an asset and those who make it the primary strategic asset to drive both decisions and outcomes. Data-driven decision-making — using big data — allows banks to gain a better understanding of the various physical, societal, financial and commercial aspects of their operating environment. This, in turn, improves the quality of decision-making, helping banks prevent financial crime, protect their reputations and create value by helping their customer-facing organizations do a better job of understanding the people with whom they do business.

The data transformation challenge is a three-step process, involving 1) understanding the data required; 2) using technology to obtain the right data; and 3) analyzing the information to transform it into insight.

Data transformation increases both the complexity of data and its potential business value. There are many ways to increase the volume and quality of data, including:

- Increasing the number of data sources (both internal and external);
- Increasing the volume of data used in financial crime investigations;
- Gathering more detail, such as more elements of the SWIFT message; and
- Using more types of data, including structured and unstructured data.

However, unless consideration is given to how to derive useful information from all of this data, it will not deliver sustainable business value.

There are tactical changes which financial services firms can make to obtain more information from data, including use of analytics techniques such as text mining. The addition of more analytics can increase the information yield from data, which may, in turn, help the organization understand the risk posed by a specific prospect, customer or transaction.

Ultimately, though, information is only useful if it can be acted upon. This means transforming information into actionable insight, and it requires alignment of processes and people along with coordination and empowerment to make use of the information.

Another problem with information is that it has a limited shelf life. It can only be turned into insight for a short time, unless there is a feedback loop of continuous improvement to inform the strategy for data collection and provision, and its subsequent transformation into information and insight. Since fraud and financial crime are always evolving, the methods for using and transforming data must advance and develop as well.

3. Applying Data Visualization Techniques

As the volume and complexity of data increase, key software providers such as SAS are adopting data visualization techniques allowing complex data to be viewed by business experts through a visual interface.

This helps the business process experts look for visual patterns and identify inconsistencies. For example, once a customer account is opened, there is continuous monitoring to flag any suspicious transactions or activities. A visual view of how transactions flow across multiple accounts helps investigators identify new patterns. When complex cases are investigated in more detail, visual clusters of the interrelated accounts assist in the analysis and identification of risks.

New and emerging technologies can be used to obtain insight from emails, chat messages or voice messages. This can help banks understand whether staff behavior is in line with expectations about what needs to be done to prevent financial crime.

Communications data, for example, can provide evidence that employees are knowingly taking on high-risk clients; that they are circumventing screening for OFAC (Office of Foreign Assets Control), prohibitions by removing data that would trigger additional checks; or that they are covering up known failings in the application of controls.

As customers increasingly interact with their bank via mobile and digital channels, the ability to accurately recognize a device and to capture data about it can be vitally important in preventing cyber-attacks.

Layering in additional data sets provided by these and other solutions does not necessarily mean replacing existing solutions, or making binary decisions at each solution point. Instead, data can be brought together either outside of platforms, in an analytical environment to optimize decisions and risk assessments, or within an existing solution. Some elements can even be taken on by a third party as a managed service to help reduce costs.

Accenture research shows that financial services organizations with more advanced financial crime prevention programs are significantly more likely to do two things: First, to effectively share knowledge and intelligence across business units and geographies, and second, to use data across all AML and fraud monitoring activities. For example, data collected about a client during Know Your Customer (KYC) due diligence can help AML or fraud detection efforts. This is an opportunity to identify high-risk entities and associations with PEPs (Politically Exposed Persons), as well as to anticipate behavior that can support decision-making regarding potentially fraudulent activity at a later date.

Similarly, cross-analysis of data captured from a customer in relation to that customer's domestic and corporate dealings with the bank may reveal significant insight about the true risk of doing business with that person.

Reaping the Benefits of Better Data Management

There are numerous other benefits associated with consolidation of data and improvements in data quality. Data consolidation, for example, supports the creation of shared services and centers of excellence that, through focused training and skills development, can maximize the capabilities of the people working in financial crime prevention.

Financial services organizations that work to achieve a single view of the customer to help detect and prevent financial crime may be able to reduce risks related to compliance and regulation, but they may also leverage their success to enhance their reputation and improve customer retention rates.

There are operational benefits to be realized, as well. Standardized enhancements in the account opening process – such as streamlining KYC due diligence – can lead to significant improvements in the customer experience. Process changes can make it easier for customers to provide their information electronically, or easier for the bank to re-use information that has already been provided. Along with enhancing the customer experience, these initiatives can also upgrade the quality of data.

Banks are seeking to ensure cyber security and to move toward new global standards as established by regulators. Data provides the greatest challenges and the most significant opportunities for banks to transform their financial crime capabilities, but using data to drive a more integrated approach requires centralization of data.

By using big data technologies to provide centralized access to data – rather than centralized storage – banks can employ analytics to obtain valuable insights and make informed decisions quickly and flexibly. Banks and other financial services firms need this kind of agility and adaptability more than ever, given the rapid evolution of financial crime and the ever-increasing stringency of regulatory requirements.

Notes

1. "The Economic Impact of Cybercrime and Cyber Espionage, Centre for Strategic and International Studies," McAfee, July 2013. Access at: http://csis.org/publication/economic-impact-cybercrime-and-cyber-espionage

2. "Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age," Ponemon Institute, August 2013. Access at: http://www.experian.com/innovation/business-resources/ponemon-study-managing-cyber-security-as-business-risk.jsp?ecd_dbres_cyber_insurance_study_ponemon_referral

3. "UK banks fear cyber attack more than the euro crisis: BoE's Haldane," Reuters, June 12, 2013. Access at: http://www.reuters.com/article/2013/06/12/net-us-britain-banks-cyberattacks-idUSBRE95B0H520130612

4. "Spend on financial crime counter measures remain strong, despite difficult economic climate for FS companies," BAE Systems press release, December 9, 2013. Access at: https://www.baesystemsdetica.com/news/spend-on-financial-crime-counter-measures-remains-strong-despite-difficult-/

5. Accenture 2011 Fraud & Financial Crime Study, published February 2011

6. Accenture 2011 Fraud & Financial Crime Study, published February 2011

7. "Using big data analytics to fight financial crime – Turning volume, velocity, variety and variability of data into insight to protect your business," Unisys, 2011. Access at: http://blogs.unisys.com/eurovoices/files/2012/06/Unisys-Using-big-data-analytics-to-fight-financial-crime.pdf

About the Author

Heather Adams is a managing director with Accenture Finance & Risk Services in London, UK. She leads the ongoing delivery and development of Fraud and Financial Crime business services, defining and developing capabilities to support clients in their fraud and financial crime prevention efforts. Heather has extensive experience in delivering large-scale complex business change for banks and has worked with senior leaders to define and implement fraud and financial crime prevention strategies to drive high performance.

About Accenture

Accenture is a global management consulting, technology services and outsourcing company, with more than 323,000 people serving clients in more than 120 countries. Combining unparalleled experience, comprehensive capabilities across all industries and business functions, and extensive research on the world's most successful companies, Accenture collaborates with clients to help them become high-performance businesses and governments. The company generated net revenues of US$30.0 billion for the fiscal year ended Aug. 31, 2014. Its home page is www.accenture.com.

15-1139