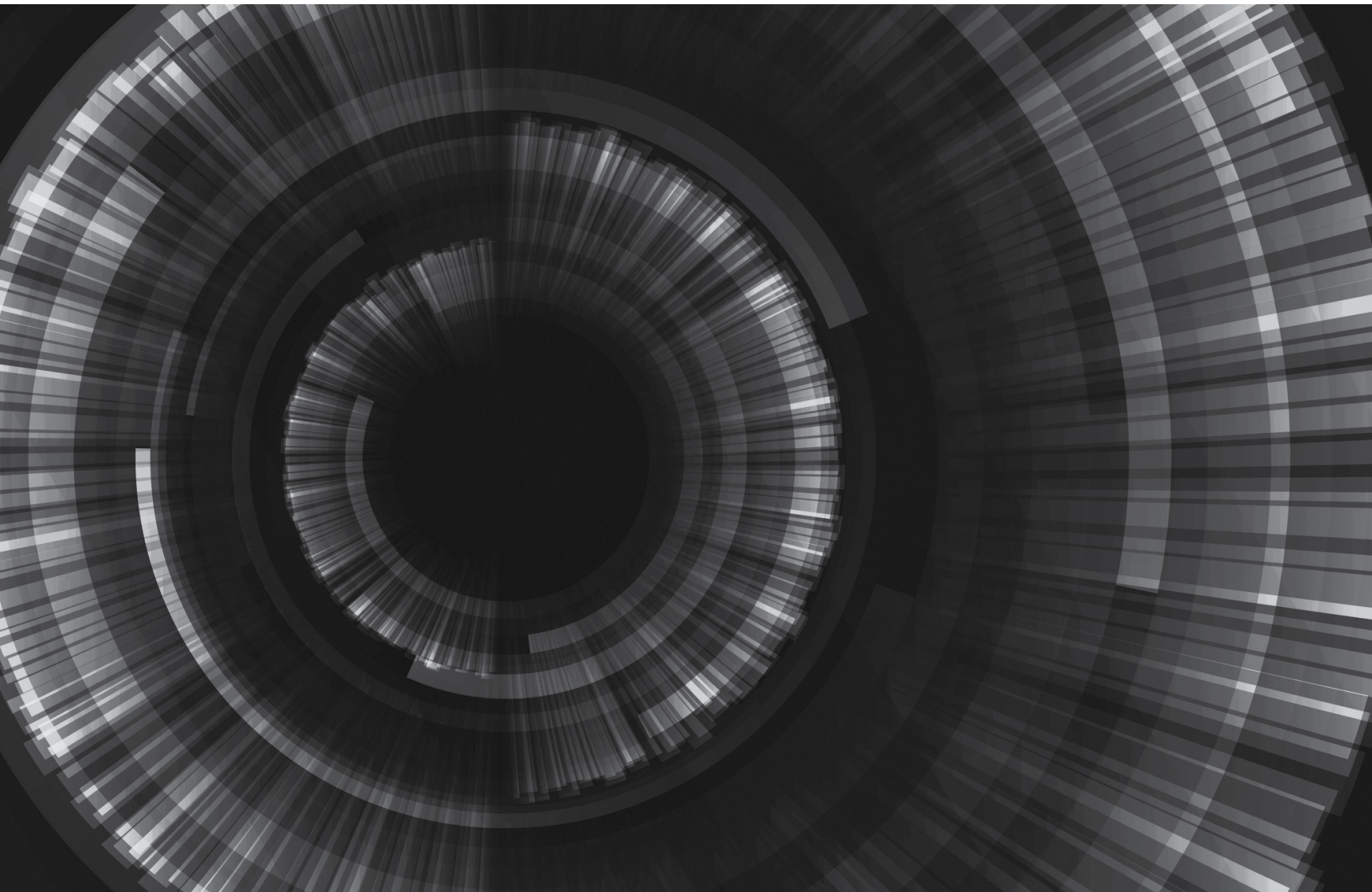
CAPCO

CAN BANKS SEIZE THE OPPORTUNITY TO COLLABORATE TO FIGHT FRAUD?



THE FRAUD LANDSCAPE

Canadians have lost over $500 million to scams from 2014 to 2018[1] and are more concerned with fraud and identity theft today than they were five years ago. This widespread concern is not unwarranted. From a rise in account takeover to the threat of authorized push payment fraud (APP), the fraud landscape is quickly evolving. In fact, the uphill battle is not expected to plateau anytime soon. Financial institutions are peering forward and bracing for a new wave of attacks led by an era of digital transformation and on-demand servicing.

Bad actors are eager to exploit the weaknesses of defense mechanisms behind these newly developed digital capabilities.

Simultaneously, payments modernization has swept through the global landscape with 'Faster Payments' in the UK, 'Instant Payments' in Europe, and the 'New Payments Platform (NPP)' in Australia. A shift to faster payments is well underway in the U.S., and Canada's real-time payment system, the 'Real-Time Rail,' is expected to follow in 2020. With new changes come new vulnerabilities and increasing threats. When the rollout of Faster Payments took place in the UK, online banking fraud alone went up a reported 264 percent within the first two years[2].

A SILOED APPROACH TO FRAUD

With an increasingly complex fraud landscape, fraudsters have banded together to form powerful organized crime rings, while financial institutions, on the other hand, have largely opted to stand solo. The fraudsters are winning and reaping the benefits of a systemic disconnect. Canada's financial institutions have traditionally used a combination of internal intelligence, business rules, and analytics to detect fraud. The reality is that these methods have been backed by data sets that are too narrow and limited in scope. Fraud watchlists used by banks are siloed, not just between competing banks, but also internally constrained by organizational boundaries. Watch lists are assembled using intelligence associated with fraudulent events after an initial breach has already occurred. Without connectivity to a shared intelligence network, there is no proactive feedback loop, enabling fraudsters to breach multiple FIs and organizational divisions undetected.

With the speed and irrevocability of real-time payments, it is more important than ever for financial institutions to access relevant and timely data. However, based on a recent survey from Forrester, roughly half of the financial services companies don't have access to real-time or actionable insights on fraud[3].
In the new age, it will become progressively more challenging for banks to continue to fight fraud independently. There is power in collaboration, and a coordinated approach can be the key to intercepting fraud and mitigating potentially billions of dollars landing in the hands of fraudsters.

THE CONSORTIUM SOLUTION

Collaborative efforts in the form of consortiums have been emerging globally to tackle critical issues across different areas such as fraud, financial crimes and cybersecurity. Commonly comprised of multiple parties across both the public and private sectors, consortiums enable their members to access a shared network of intelligence that can be used to augment existing data, improve predictive models, and deliver critical new insights that would have otherwise been unavailable.

Geo	Consortium	Founded	Description
United Kingdom	Credit Industry Fraud Avoidance System (CIFAS)	**1988**	A non-profit organization and fraud prevention service with the largest database of instances of fraudulent conduct in the UK. Organizations from across sectors share their data to collaboratively reduce instances of fraud and financial crime. CIFAS has been claimed as the world's first fraud data sharing scheme and the closest thing the UK has to a national fraud database[4].
	Cyber Security Information Sharing Partnership (CiSP)	**2011**	Consisting of members across government and industry, CiSP is a social networking platform hosted on the internet that allows members to exchange cyber threat information in real-time, in a secure and dynamic environment, while protecting the confidentiality of shared information.
	Cyber Defence Alliance (CDA)	**2016**	Founded by Barclays, Standard Chartered, Deutsche Bank, and Banco Santander, the CDA enables members to share information with each other regarding tactics used by cyber-crime groups targeting the financial sector, and to collaborate in an intelligence analysis environment in the fight against cyber fraud and financial crimes. Other major UK banks and law enforcement agencies have since joined the consortium.
United States	Financial Services Information Sharing and Analysis Center (FS-ISAC)	**1999**	A non-profit association dedicated to protecting financial services firms from physical and cyber-attacks. It brings together banks, government agencies, and law enforcement agencies to collaboratively share intelligence anonymously and has been instrumental in defending against threats such as account takeover, fraud, and ransomware.
	Early Warning Services (EWS)	**2006**	An alliance initially formed between Bank of America, BB&T, JP Morgan Chase, Wachovia, and Wells Fargo to bring together fraud prevention expertise. EWS leverages relevant technology and consortium data to help financial institutions and businesses assess risk and fight identity and payment fraud.
	CyFin (Program from The National Cyber-Forensics and Training Alliance)	**2007**	Established for the purpose of disrupting cyber threats to the financial services industry, specifically targeting incidents such as account intrusion, fraud, identity theft, and money laundering. Members come from across several industries such as banking, insurance, and payments.
Europe	Europol Financial Intelligence Public Private Partnership (EFIPPP)	**2017**	The first transnational financial information sharing mechanism comprised of experts from financial institutions and government authorities in seven European nations and the U.S. Its objective is to facilitate the exchange of strategic, operational and/or tactical intelligence associated with ongoing investigations for financial crimes. The organization also supplies banks with data on risks posed by correspondent accounts as part of a new initiative aimed to tackle fraud and money laundering.
Australia	Australian Financial Crimes Exchange (AFCX)	**2016**	A non-for-profit organization formed by Australia's four major banks to combat financial-related crimes. It provides a secure environment for sharing and accessing financial crime data and intelligence. Member banks collaborate with each other, alongside regulators and law enforcement agencies to detect trends and collaboratively shut down fraudsters.

THE CONSORTIUM SOLUTION (CONTINUED)

In the UK, consortiums have been around since the birth of the Credit Industry Fraud Avoidance System (CIFAS) in 1988, one of the largest shared databases of fraud intelligence in the country. From 2005 to 2010, members ranging from financial institutions to private companies of various sectors have reported a total of £4.2 billion of fraud prevented through CIFAS. Members saved £268 of fraud for every £1 of the subscription membership fee that was paid[5]. Another early example of data silo disruption includes the efforts of the Financial Services Information Sharing and Analysis Center (FS-ISAC) formed with encouragement from the U.S. government. Its most significant collaborative moment occurred with the formation of the Account Takeover Task Force (ATOTF), from 2009 to 2010, a period when the financial services industry saw a huge uptick in ATO attacks. Financial services firms, industry associations, processors, and government agencies worked together on prevention and detection, and in one year, saw a 36 percent drop in the number of ATO attacks involving a loss of funds[6].

More recently, banks themselves have been coming together to explore the benefits of industry-wide collaboration. In the U.S., a group of leading banks rallied together to form Early Warning Services (EWS), based on their shared belief that fraud should not be a competitive issue. Focusing on the fight against identity and payment fraud, EWS has a data exchange system that enables members to share intelligence and collaborate on fraud prevention. Similar alliances have emerged in other parts of the world. In response to a rise in major security incidents in the UK such as the attack on Tesco Bank in 2016, the country's biggest financial cyber heist, top banks came together to form the Cyber Defence Alliance (CDA). Initiated by Barclays, Standard Chartered, Deutsche Bank, and Banco Santander, the CDA enables members of the alliance to share information and experiences to prevent the ever-increasing number of cyber-attacks on financial organizations. Meanwhile, in Australia, the country's four major banks have formed the Australian Financial Crimes Exchange (AFCX), a forum that enables members to share, access, and download anonymous financial crime data.

Canada has remained relatively reserved when it comes to the topic of consortiums, particularly among the banks. However, the idea of industry-wide collaboration is slowly gaining traction with organizations such as CANATICS bringing competing insurance companies together to achieve a common goal. Many of Canada's facilitators of money movement like Interac and the credit card rails have leveraged their data to protect the system and provide fraud alerts and services back to participating FIs. Compared to its global peers, Interac has some of the lowest levels of skimming related fraud losses to financial institutions. In 2018, Interac reported annual losses were down to only $4.4M in 2018[7] as a result of not only their chip and pin technology but also their monitoring which cuts across data from all FIs in their eco-system. However, while these fraud prevention solutions are effective, they remain within a product or service silo.

Canadian banks are slowly moving the dial forward with collaborations with industry players such as Symcor and their COR.IQ suite of fraud consortium products.

SPOTLIGHT ON CANADIAN NATIONAL INSURANCE CRIME SERVICES (CANATICS)

Comprised of major insurance providers operating in Ontario, CANATICS leverages a shared pool of industry data and analytical capabilities to reduce auto insurance fraud. While CANATICS is unique in Canada, it is one of a growing number of Insurance anti-fraud consortiums around the world which is quickly becoming a leading global practice. Insurers were keen to band together, primarily because of the data enrichment opportunities from other insurers and also valuable government and healthcare data. The rich data set has allowed for the proactive detection of organized fraud rings that target multiple insurance companies at a time to fraudulently collect claims money.

Ben Kosic, President and CEO of CANATICS has some advice regarding a fraud consortium for Canada's banks, "This is a huge opportunity that many don't realize. It will make a material difference. Fraudsters are organized, and while it is difficult to be a step ahead, you don't need to be five steps behind them if you collaborate." Ben recommends the banking industry, 'be bold' and manage their risk aversion to sharing and using data. Ben also recommends working with the government to generate a 'safe harbor' for the use of data for fraud. In today's age, where customers are moving more and more to disintermediated straight-through processing, fraud monitoring should be looked at as an accelerator for good customers.

According to Ben, you can leverage leading edge anti-fraud services as mechanism to identify good customers and accelerate their experience while decelerating the bad actors and attempting to get ahead of the payment.

BARRIERS AND CHALLENGES TO CONSORTIUMS

Despite the benefits of consortiums, why have Canadian financial institutions remained reluctant to share and collaborate in the fight against fraud? From a business perspective, the idea of data consortiums brings forth a stream of questions: What will be the return on investment? Will the consortium result in more significant benefits for our competitors? In the case of FS-ISAC, information sharing began very slowly and took as long as 18 years for the process of information sharing within a community to take hold among financial institutions. There are also associated privacy concerns when it comes to sharing information. One of the major areas of differentiation and inherent values shared by traditional financial institutions is their dedication and proven competency in data security. Combined with heightened consumer demands for privacy, banks are more careful than ever before when making decisions about sharing customer information.

Financial institutions with even the most progressive attitudes towards fraud consortiums can run into internal capacity challenges. Banks have a multitude of on-going projects at a given time, many of which support critical business activities that are often deemed higher in priority.

Recently, Symcor, a service provider to Canada's top FIs, announced a suite of fraud solutions, COR.IQ, designed to leverage the power of consortium data to produce an extensive set of fraud signals, enhanced and verified through AI.

BARRIERS AND CHALLENGES TO CONSORTIUMS (CONTINUED)

Multiple Canadian banks have now signed on to COR.IQ. Symcor's Head of New Product & Innovation, Saba Shariff believes that now is the right time for Canadian FIs to leverage the advantages in collaboration and consortium data. "There's no doubt that banks are committed to better fraud prevention and detection for their customers. However, whether your customers are good or bad, can't fully be answered within a single FI. An alliance amongst multiple Canadian FIs provides a line of sight that a single FI can't get a view of – fighting fraud shouldn't be seen as a competitive advantage."

Shariff recognizes the industry has tried before; however, she believes you need a neutral third-party to enable that. "Infrastructure is costly and resources are scarce making now an ideal opportunity to collaborate and consolidate." She believes Symcor's road to get there is easier than many organizations. "Given our history as a trusted custodian of data, we have successfully expanded our fraud offerings which started with duplicate cheque, flagged accounts and counterfeit cheques and now moving towards image-based solutions and entity-related."

KEYS TO SUCCESS

Drawing on the experiences of global consortiums, and considering the modern challenges faced by Canadian financial institutions, there are best practices that can be put in place to form an effective fraud consortium.

1. **A trusted third-party governing body** must be present to ensure that participating members enter into a mutually beneficial agreement based on shared values. Equal participation and contribution will need to be managed regularly, and the appropriate metrics defined to measure a consortium's on-going success. These activities are critical to mitigating potential breaches in trust and increasing the confidence of members for successful collaboration.
2. **Bilateral Agreements to share data for fraud** – consortium members should all agree to collective bilateral agreements with the centralized third party to facilitate the use of data for identification of fraud. This will empower financial institutions to participate and contribute valuable intelligence while mitigating concerns that come with greater transparency.
3. **Effective data strategy** – The consortium will require a platform that confidently ensures data shared over the network is secure and protected. From the lessons learned from CANATICS, Ben Kosic recommends working with a secure provider to host the data, however, don't disintermediate the consortium team from the data. Enable the analytics team within the consortium to quickly produce new analysis and models.
4. **A cultural shift** – to be successful, Kosic also recommends financial institutions must think differently about collaborating :
   - **a.** Dont compete to shift fraud around.
   - **b.** Collaborate to reduce the size of the fraud pie.
   - **c.** Collaborate through all phases of the fraud lifecycle (deterrence, detection, investigation, and action – including meaningful consequences.)

Now is the time for financial institutions to leap forward and collectively move towards a new age of fraud prevention where banks take one step forward, and fraudsters take two steps back.

REFERENCES

1. https://www.theglobeandmail.com/business/adv/article-advancing-awareness-on-how-to-recognize-reject-and-report-fraud/
2. Financial Fraud Action UK Annual Review: Working Together to Prevent Fraud. London: Financial Fraud Action UK, 2015.
3. https://www.transunion.ca/blog/id-fraud-management#_ftn2
4. https://governmentbusiness.co.uk/features/sharing-fraud-data-prevent-further-fraud
5. Peter Hurst, "Sharing fraud data to prevent further fraud," 2010, https://governmentbusiness.co.uk/features/sharing-fraud-data-prevent-further-fraud
6. William Nelson, "The Value of Information Sharing," n.d., https://www.theclearinghouse.org/banking-perspectives/2017/2017-q2-banking-perspectives/articles/the-value-of-information-sharing
7. https://www.interac.ca/en/fraud.html

AUTHORS

Joanna Lewis, Partner
Nebojsa Cukilo, Principal Consultant
Jennifer Dong, Consultant

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at www.capco.com, or follow us on **Twitter**, **Facebook**, **YouTube**, **LinkedIn** and **Instagram**.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Hong Kong
Kuala Lumpur
Pune
Singapore

EUROPE
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO