Stronger Together

Why collaboration is the best first step in fighting fraud

Insights from Interac Corp.

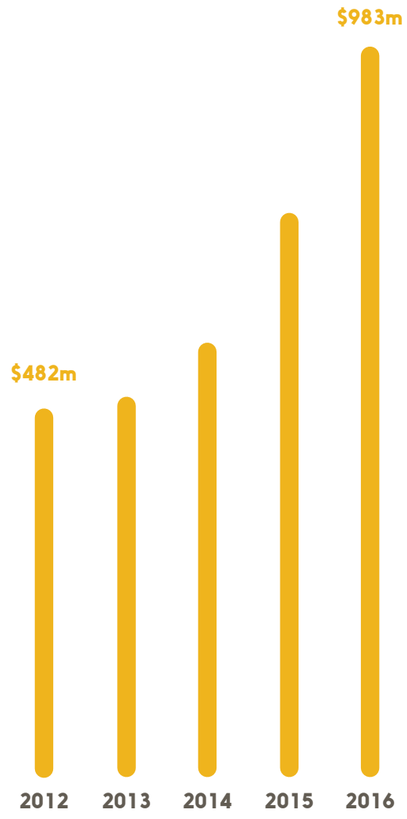
"We are firmly committed to playing our part in ensuring that consumers have safe and secure access to their money and that financial crime risk is never a barrier to them adopting new products and technologies."

Introduction

The last two decades of technological innovation have ushered in a new world of unprecedented connectivity and convenience. In financial services, customers have never before enjoyed such easy access to their money, whenever and wherever they might need it – nor has it ever been so simple to transfer money between family and friends or to make purchases digitally, connecting people, businesses and governments alike.

Such accessibility and ease, however, have come with a much less welcome side. As has happened with every other innovation in banking throughout history, ill-intentioned actors have used the power of technology to devise new ways of committing fraud. The rise of e-commerce, for example, has opened avenues for "card-not-present" fraud, in which a criminal uses stolen card data – without needing the card itself – to purchase goods and services. In Canada, total gross fraud losses on Canadian customer accounts surpassed $980 million in 2016, while in the United States in the same year, losses totaled $7.7 billion – an amount projected to reach $12 billion by 2020.*

At Interac, we are firmly committed to playing our part in ensuring that consumers have safe and secure access to their money and that financial crime risk is never a barrier to them adopting new products and technologies. We design our products with security and customer experience at the forefront. As such, fraud prevention has been a key focus of our efforts, as we work closely with our financial institution partners, merchants, consumers and law enforcement in an ongoing program of risk reduction and trust-building. In this white paper we'll discuss the main principles behind this work.



A growing problem

During the five year period from 2012 to 2016, total gross fraud in Canada more than doubled.* Over 95% of this total is attributable to credit card fraud.

* Sources: Statista.com, Canadian Bankers Association, Interac Corp.

Everything starts with trust

Fraud exploits and erodes trust, and this has a significant negative impact on the smooth operation of the economy

Money, famously, is a society-wide exercise in trust sustained over decades and centuries. A loonie isn't worth much as a round piece of metal alloy, but as "a dollar" we know what it can be traded for. Most of our monetary wealth isn't physical at all, but simply entries in digital ledgers stored on financial institution servers. We trust our financial institutions to give us our money when we ask for it, and we trust merchants to hand us our purchases after we've paid for them. In the absence of trust, we'd be back to a primitive barter economy. I'll give you three goats for that wheelbarrow.

Fraud, at the root, exploits and erodes trust, and this has significant negative impact on the smooth operation of the economy, as well as on the day-to-day interactions between companies and consumers. A financial institution that trusts a customer can authorize higher value transactions, like a mortgage or a business loan – a situation that obviously benefits the financial institution, the customer, and the economy itself. And with customers there's a virtuous circle too, because when a customer trusts their financial institution, they are much more likely to take advantage of tools made available to them to help stop fraud and protect their own money – tools like transaction monitoring, email and text alerts, credit freezes, and so on.

It is in the best interest of financial institutions, merchants, and their partners to work together, sharing information for the purpose of increasing trust and mitigating fraud risk. Although some of these actors are natural competitors in the marketplace, the benefits of collaboration far outweigh the risks.

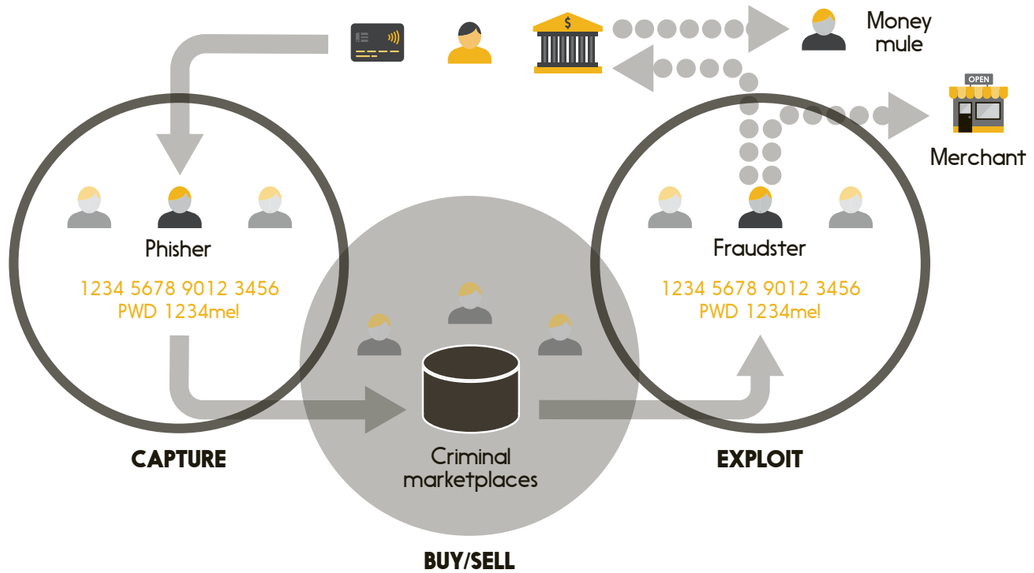
Why standing together is better than standing apart

There's a reason you find herbivores collected in large groups: if they grazed alone, predators would find it trivially easy to catch and eat them. That's not because a single wolf, for example, is more than a match for a single caribou. It's because wolves work together, and if the caribou don't band together in response – all eyes on the tree line, all animals alert to signals from other herd members – then the wolves will win.

The same technology that enables easy access to goods and services also enables easy alliances between criminals. The lone hacker in a bedroom – vivid though this cultural image still is for us – is no longer representative of the threat that our financial system faces. Although some lone wolves still operate and are successful, we often find that fraud is committed by networks of criminals, connected digitally and often organized based on their individual specialties: those who capture highly sensitive and valuable data, such as card numbers, usernames and passwords; those who sell it on black markets; and those who purchase and exploit that data for financial gain, often stealing money from unsuspecting customer accounts.

Dark networks

Fraud is committed by underground networks of criminals, each of whom has a specialty; perpetrators don't even need to meet each other in person.



Perpetrators don't even need to meet each other in person: in the same way that online consumer marketplaces made trust measurable through their reputation engines, criminal platforms used by hackers and fraudsters offer their own rating systems. In fact, while the rest of the world is just now coming to grips with the possibilities of "the collaborative economy", criminals were amongst its earliest adopters.

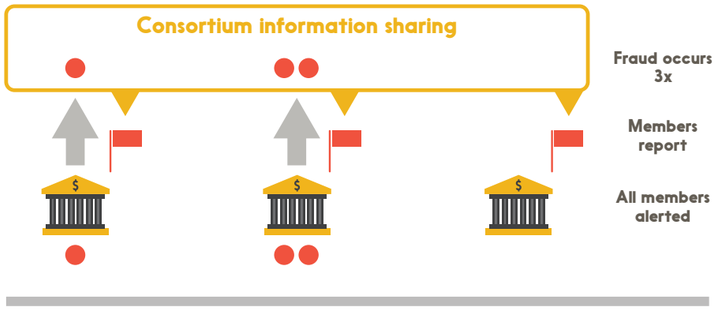
By trusting each other and organizing virtually, today's criminals are able to mount very complicated fraud schemes, impacting (or exploiting) multiple financial institutions, and are not bound by physical borders.

Our response to this must be equally coordinated and firm. Consider two hypothetical situations.

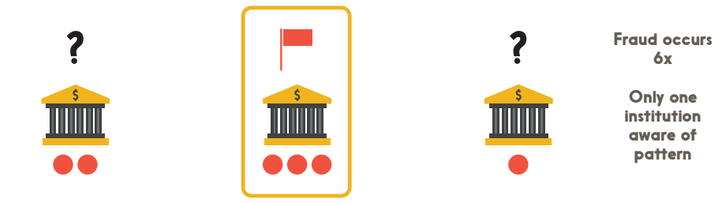
In the first, financial institutions fight fraud alone and do not share information with each other. For a single institution to notice a fraud scheme underway, its own customers would have to be targeted multiple times for a pattern to emerge – something that might take some time in a scheme that targets the customers of many banks. In the second case, where the right kind of information is shared between institutions, a fraud scheme targeting just a handful of customers across several banks might be enough to establish a pattern – thus enabling action to be taken much sooner to stop the scheme from going further.

Forewarned is forearmed

In a consortium that shares information about fraud activity, not only will fraud patterns get flagged faster, but all consortium members will be alerted immediately — including those who haven't yet experienced the fraud.



In a "siloed" system, a financial institution must wait for a pattern to reveal itself through multiple frauds against its own customers — and other institutions won't benefit from any forewarnings, remaining vulnerable.



The best defence has layers

Our fraud strategy aims to drive fraud out of Canada by focusing on efforts to **prevent** the capture of data needed to commit fraud, **detect** exploitation, and **respond** to areas of higher than average risk.

True effectiveness on all three fronts requires a range of activities. Prevention depends not just on technology, but on smart product design and on education. Detection is enabled through continuous monitoring, pattern recognition, and timely alerts. Response, in turn, is a mix of planning, coordination, and engagement with law enforcement.

These are continuous, ongoing activities that require the uninterrupted attention of organizations, and the active participation of all parts of the financial and commercial ecosystem: financial institutions, networks, merchants, and consumers.

As a transaction-oriented network, we've been able to play a key role in a consortium-based approach to combating fraud. Because we connect financial institutions to each other – and to merchants and customers – we've been able to act as a point of cross-system awareness and coordination. The customers of both the *Interac*® Debit and *Interac* e-Transfer® platforms have benefitted from our monitoring and analysis of transactions and their patterns, as well as from their own fraud reporting and other feedback loops of information that allow institutions to benefit from the early warning signals that their peers are providing. All this is achieved not by pooling everyone's data – but rather by sharing just enough relevant information to enable the monitoring of suspicious or anomalous activity and to trigger investigation and action – by the network, by the financial institutions, and often by law enforcement.

Collaboration wins

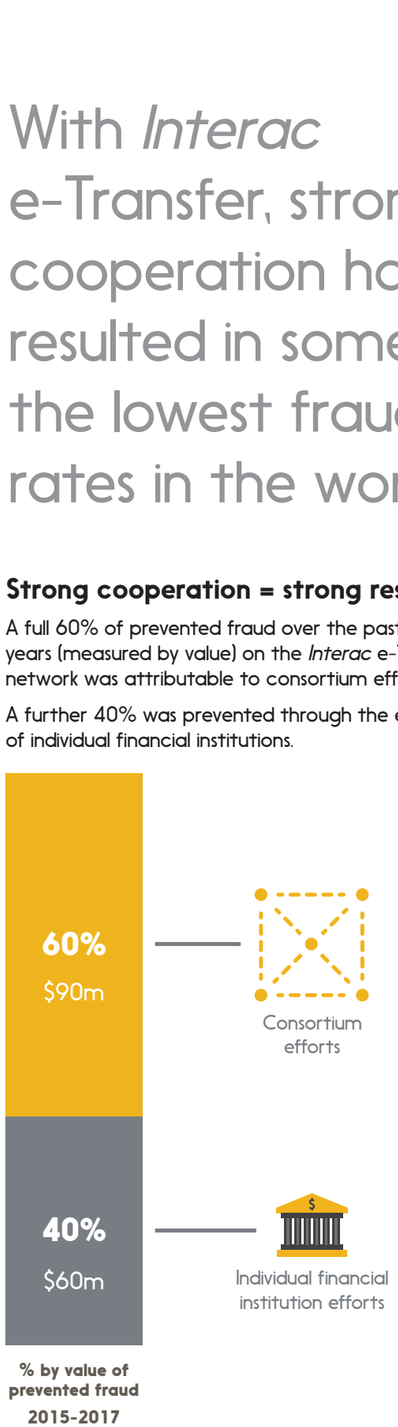
Because of industry-wide cooperation involving both new technology and information sharing, fraud on the *Interac* Debit network has been reduced to its lowest levels in history.

With *Interac* e-Transfer, strong cooperation has resulted in some of the lowest fraud rates in the world

Strong cooperation = strong results

A full 60% of prevented fraud over the past three years (measured by value) on the *Interac* e-Transfer network was attributable to consortium efforts.

A further 40% was prevented through the efforts of individual financial institutions.



Source: Interac Corp.

Information sharing, though, is not enough. The strongest defence is a layered defence: one in which each participant does their best to combat fraud within the scope of their own abilities, and in which each participant supports the others in their efforts, so that the system as a whole is as resilient as it can be.

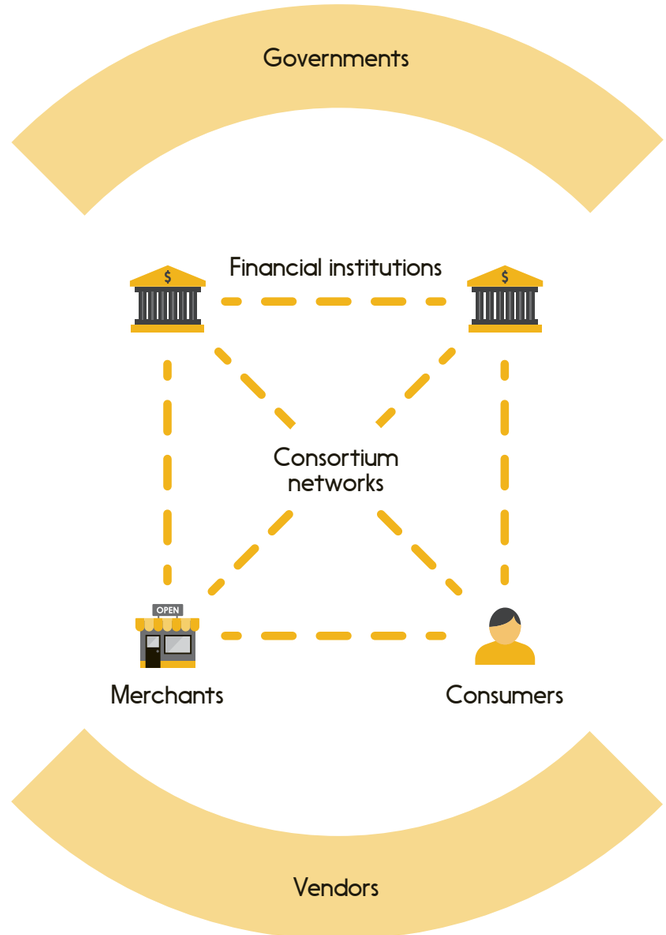
Because *Interac*-branded debit cards are used in physical locations across the country to purchase goods and services, for example, we place emphasis on ensuring that merchants in our network have the tools and knowledge they need to identify and prevent fraud at the point of sale. As more transactions move to smartphone devices, new technologies such as tokenization further abstract a user's personal account number with a randomized account number (or "token") useful only for the transaction and useless to hackers or identity thieves. Finally, we arm consumers themselves with technology (chip-and-PIN secured debit cards, for example) and with education designed to minimize their chance of falling victim to fraud – and, by extension, to maximize the trust they're able to place in their financial institutions and in the merchants they shop with.

In a similar vein, financial institutions must continue to focus on ensuring that their own customers do not fall victim to fraud (nor able to commit fraud, for that matter) by implementing the best practices and technologies available for authentication, monitoring, and rapid response. Interac acts as a force multiplier, helping increase the overall effectiveness of industry efforts by deploying consortium measures.

Here in Canada, such measures are best exemplified by *Interac* e-Transfer, where strong cooperation has resulted in some of the lowest fraud rates in the world, in large part due to the spirit of collaboration that has been achieved amongst our partners. Although there will never be a single security measure that will stop fraud and identity theft completely, one of our strongest defences is a layered system of collaborators: each independent, all connected.

Everyone participates

Fraud can only be stopped with the active participation of all players in a financial/commercial system: safeguarding data and personal information, detecting frauds as or soon after they occur, sharing relevant information, and taking fast and effective action — everyone has multiple roles to play.



Toward a safer future

Success certainly doesn't mean we can just rest on our laurels. Technology marches forward, and almost every new innovation opens up additional vectors of attack for criminals to exploit. We must continue to design products with security in mind, to have the right controls in place to detect fraudulent activity when the bad actors find a loophole, and to be ready with a coordinated and relentless response.

As an industry, we need to continue honing our collective skills and capabilities – not just technical, but organizational and collaborative ones, so that new attacks are only surprising the first time they occur, never the second. Together, we can provide security to our customers and put criminal networks on the defensive.

In our future whitepapers and blog posts we will explore in more depth the challenges, initiatives, and successes of our collective fight against financial crime.

"As an industry, we need to continue honing our collective skills and capabilities – not just technical, but organizational and collaborative ones."

For more information on this topic, visit innovation.interac.ca

Published April 2018