

CCAO Annual Report

Customer Complaint
Appeal Office



ABOUT US - WHO WE ARE

The Customer Complaint Appeal Office (CCAO) is the third and final step in BMO's Canadian Complaint Handling Process. The CCAO provides customers an opportunity to appeal concerns that have not been resolved in either of the first two steps of BMO's Complaint Handling Process. The CCAO does not report directly to any business area and is not involved in BMO's business operations.

Our mandate is to review unresolved customer complaints by applying a dispute resolution process that is accessible, fair, and transparent. Although we have a broad mandate to review a wide range of financial services complaints, there are certain issues that fall outside of our scope. These matters typically include business, credit and risk management decisions, and matters that are before a court.

During our reviews, we often identify opportunities and make recommendations on how BMO can provide better customer experience or improve operations, products, or services.

For additional information, please refer to our website [Customer Complaint Appeal Office - Our Impact \(bmo.com\)](https://www.bmo.com/ccao)

WHAT WE DO - OUR PROCESS

We review unresolved Canadian customer complaints, involving banking products and services (BMO Bank of Montreal), investment products (BMO Nesbitt Burns, BMO InvestorLine, BMO Investments, and BMO Private Banking), and insurance products (BMO Insurance, BMO Creditor and Travel Insurance, and BMO Estate Insurance Advisory Services).

Our process begins once a customer has completed the first two steps of [BMO's Complaint Handling Process](#).

See the next page for full process details.

About us – Who we are
What we do – Our process
2023: A year in review
Fraud & scams
Fraud & scams: Examples
How to protect yourself
Contact us



1

ACKNOWLEDGE RECEIPT OF COMPLAINT

We acknowledge receipt of the complaint and provide the customer with details of the review process and next steps.



2

SCOPE

We perform an initial review to determine if the complaint is within CCAO’s scope to change the outcome (e.g., CCAO does not reverse or alter credit decisions or risk management decisions or review matters before the court).



3

REVIEW

In-scope complaints are assigned for review. Depending on the nature and complexity of the complaint, the review may require:

- Additional information from the customer and internal business groups.
- Review of internal policies, phone calls, research external sources and interviews.
- Review of documentation and records, specific transactions, and account history.
- Review of the customer’s overall experience.



4

OUTCOME

Our review concludes with a written response that may include a recommendation to resolve the complaint, re-extension of a previous offer made by the line of business or a decline that supports the business decision to take no further action on the complaint and close the matter.



5

ESCALATION

If we have not responded to the complaint within 56 days for banking matters or 90 days for investment matters from the date the complaint was first received by BMO Financial Group, or the customer remains dissatisfied, the next available option is to escalate to an external complaints body: The Ombudsman for Banking and Investment Services (OBSI) for external reviews of banking and investment complaints and OmbudService for Life & Health Insurance (OLHI) for insurance-related complaints.

FAST FACT

In 2023, OBSI completed over 700 reviews and agreed with BMO’s decision 92% of the time, while OLHI completed 2 reviews with 100% agreement.

About us –
Who we are

What we do –
Our process

2023:
A year in review

Fraud & scams

Fraud & scams:
Examples

How to protect
yourself

Contact us

2023 – A YEAR IN REVIEW

Our office completed 2,587 reviews (2,545 related to banking and 42 related to investments), up 104% compared to 2022. 65% of banking complaints were resolved to the satisfaction of the customer. The average time for BMO to complete a review was 47.5 days, which represents the total number of days end-to-end, less any time that the customer was inactive with us.

On the investment side, most complaints related to service issues, account transfers, suitability of investments, and fees. 50% of complaints were resolved to the satisfaction of the customer.

In 2023, we handled a significant number of complaints from customers who fell prey to third party scams, some of whom were tricked by third parties into clicking on links and sharing their personal information (knowingly or unknowingly) through deceptive emails, text messages and phone calls, and subsequently large sums of money were removed from their accounts.

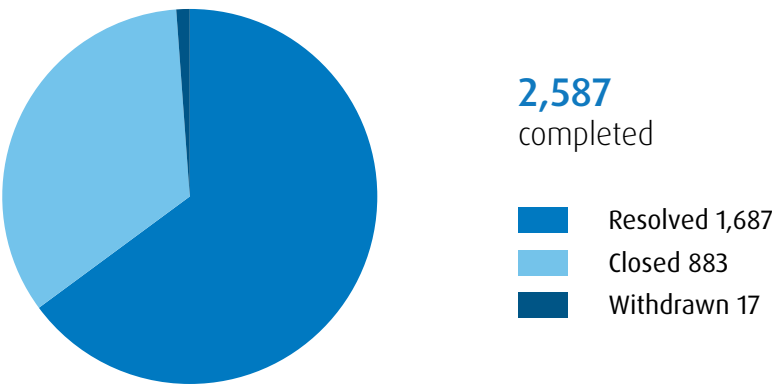
Like handing car keys to a thief, providing personal information (e.g., bank card number, PIN, authentication codes etc.) to a third party (scammer) for any reason circumvents BMO’s efforts to protect customers from fraud. In most cases, scammers disappear with the money so quickly that recovery of the stolen funds is not possible, leaving the customer responsible for the loss. BMO will only reimburse on complaints where the customer has not contributed to the loss by providing personal information whether knowingly or by mistake. BMO does not have funds set aside to reimburse customers that provide their personal information to a third party.

Against the challenging economic backdrop, of 2023, these financial losses were difficult for our customers.

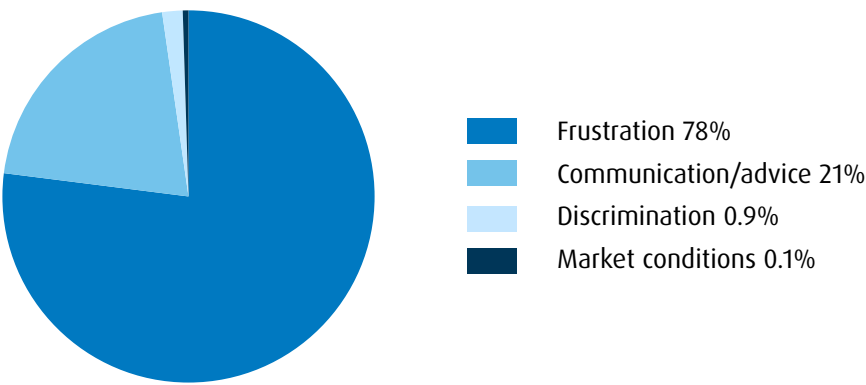
FAST FACT

Approx 57% of the complaints reviewed in 2023 were related to fraud, of which over half related to third party scams.

COMPLAINT REVIEWS BY OUTCOME



NATURE OF COMPLAINTS



About us –
Who we are

What we do –
Our process

2023:
A year in review

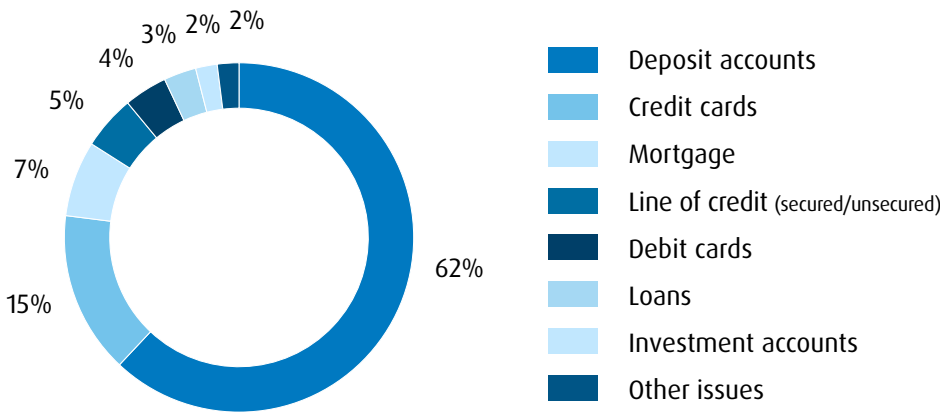
Fraud & scams

Fraud & scams:
Examples

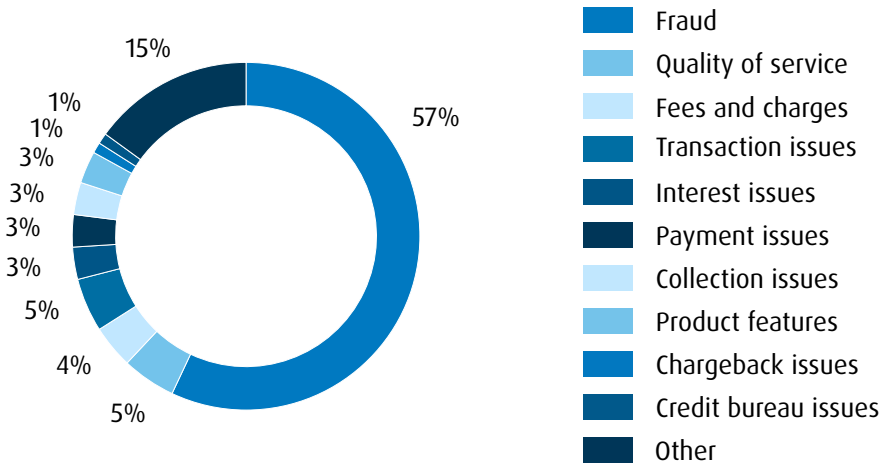
How to protect
yourself

Contact us

COMPLAINT REVIEWS BY PRODUCT



COMPLAINT REVIEWS BY SERVICE



FRAUD & SCAMS

Securing the personal information of our customers is our priority. Customers must also to do their part to help keep their personal information safe. BMO provides a Digital Banking Security Guarantee that states that we will reimburse for any eligible unauthorized transactions provided the customer has kept their account details secure and has met all other key responsibilities outlined in our Electronic Banking Services Agreement. Regrettably, sometimes customers are not aware of how they have been compromised, and thereby given away their account details.

The Digital Banking Security Guarantee does not apply to complaints involving scams where customers knowingly or unknowingly give away their information to a third party. We see situations where scammers entice customers to click a link or download an attachment that installs malicious software (also known as malware) on their device, which then allows the scammer full access to any/all information available within that device. We also know that the time between device infection and the scammer accessing a bank account can vary from minutes to months which can make it difficult for customers to identify the exact point of compromise.

It is prudent for customers to educate themselves on scams targeting Canadians by visiting the Canadian Anti-Fraud Centre (antifraudcentre-centreantifraude.ca), as many of these scams involve customers giving away their information, which results in them being ineligible for reimbursement.






WHEN CAN BMO HELP?

Reimbursement possible

Under BMO’s Digital Banking Security Guarantee BMO will reimburse when a fraud has occurred, and the customer has not contributed to the loss by providing personal information, knowingly or unknowingly.

Reimbursement NOT possible.

Under BMO’s Digital Banking Security Guarantee BMO will not reimburse where customers are convinced to authorize a financial transaction or willingly supply personal information to gain access to email and/or financial accounts.

About us – Who we are	<p>IMPORTANT: BMO will never contact you via unsolicited email, text or phone call asking for sensitive information, passwords, PINs or verification codes (one-time passcodes). If you get a call, voicemail, email or text from someone claiming to be from BMO and you think it’s suspicious, do not share any personal information and contact us immediately using the information on the back of your card.</p> <p>Here are some of the most common scams we’ve seen in 2023, which were ineligible for reimbursement:</p>	
What we do – Our process		
2023: A year in review		
Fraud & scams		
Fraud & scams: Examples	<div><p>BMO IMPERSONATION SCAMS</p><p>This scam involves a third party impersonating a BMO bank employee and convincing the victim they are helping with a bank investigation.</p><p>IMPORTANT: BMO will NEVER ask a customer to withdraw money, purchase a gift card, perform a transaction or ask for banking information including passwords to help in a fraud or internal investigation of any kind.</p></div>	<div><p>CRYPTOCURRENCY INVESTMENT SCAMS</p><p>Scammers leverage the market interest in cryptocurrency (crypto) to lure investors into scams. Some crypto investment scams are variations on traditional scams, such as investment or romance scams. Here are scams unique to cryptocurrency:</p><ul style="list-style-type: none">• Customers are directed to a specific trading platform to convert their funds into crypto assets, and then encouraged to transfer these assets to an investment website to fund an “account,” but the website and account are fake.• Customers are instructed to download software to supposedly facilitate asset conversion and transfer, but the software provides fraudsters with remote access to their personal computer.• Using false statements and the illusion of rapid gains, scammers encourage customers to make additional deposits. Ultimately, requests to withdraw the assets fails and scammers stop replying to communications, resulting in the customer losing all their funds.</div>
How to protect yourself	<div><p>PHISHING, SMISHING, AND VISHING</p><p>Fraudulent emails or fake websites (phishing), SMS text messages (smishing) and phone calls (vishing) all share the same intention: to steal personal information. Customers must be cautious when receiving unsolicited emails or messages and must NOT click on suspicious links in emails or texts, or on social media.</p></div>	<div><p>MERCHANT SCAMS</p><p>Scammers reach out via phone, email or text messages claiming that customers are owed refunds from recent purchases. Most people are excited to hear they are receiving a refund, so they click on the link or provide personal information. Before taking any action, customers should contact the merchant directly to verify the request.</p></div>
Contact us	<div><p>CANADA REVENUE AGENCY SCAMS</p><p>These scammers claim to be from the Canada Revenue Agency (CRA) and target taxpayers, requesting personal information such as a social insurance number (SIN), credit card number, bank account number, or passport number. These scammers may insist that personal information is needed so that a refund or a benefit payment can be issued. Before taking any action, customers should contact CRA directly to verify the request.</p></div>	

About us – Who we are
What we do – Our process
2023: A year in review
Fraud & scams
Fraud & scams: Examples
How to protect yourself
Contact us

HOW TO PROTECT YOURSELF

Be Skeptical

If something seems too good to be true, it probably is.

Be Inquisitive

Verify names, facts and details by doing your own research.

Be Thorough

Double check the validity of the request by talking over the phone or meeting in person. Always seek professional investment advice.

HABITS

NEVER share your bank card information.

Never give out your card, expiry date, CVV (certified verification value) or PINs to anyone, either online, via phone, or to someone who comes directly to your home.

Slow down.

Avoid any ‘urgent’ requests and be mindful of responding too quickly. Instead, take a moment to investigate, call someone you trust and then quickly follow up with the company using information directly from their website.

Review emails and URLs carefully.

Emails and websites can look like they are from trusted companies, but if you review the email and URL carefully, you’ll notice a small difference, for example, one extra letter, a period, or a .net instead of .com.

Say no to unsolicited calls, emails or visitors to your door.

If you’re unfamiliar with the caller, sender, or visitor, proceed with caution or avoid altogether.

Do your research when considering cryptocurrency and traditional investments.

Validate the investment firm’s reputation or the representative’s professional background with your own independent research. Beware if the investment representative encourages you to download specific software.

CUSTOMER COMPLAINT CONTACTS

Email: complaint.appeal@bmo.com

Phone: 1-800-371-2541
Fax: 1-800-766-8029

Mail: 1 First Canadian Place,
P.O. Box 150
Toronto, ON M5X 1H3

Visit: bmo.com/customercomplaintappealoffice