The Canadian Catholic Financial Administrators Meeting

Colin Robertson,
Chief Underwriting Officer and Vice President Risk Control

Jane Williamson,
Vice President, Claims

Rob Jordan,
Vice President, National Accounts

May 31, 2023

Today’s Agenda

1. Employee Dishonesty and Fraud
2. Social Engineering Fraud
3. PSA Trends & E-Learning
4. Arson
5. Risk Management
6. Building Inflation
7. Providing More Value

Employee Dishonesty and Fraud

Scenario 1

1. 55-year-old woman accused of stealing more than $30,000
2. Prosecutors contended that the woman used her position as a volunteer church treasurer to write checks to herself and make withdrawals from church accounts
3. She had held the position of treasurer for over 25 years

Scenario 2

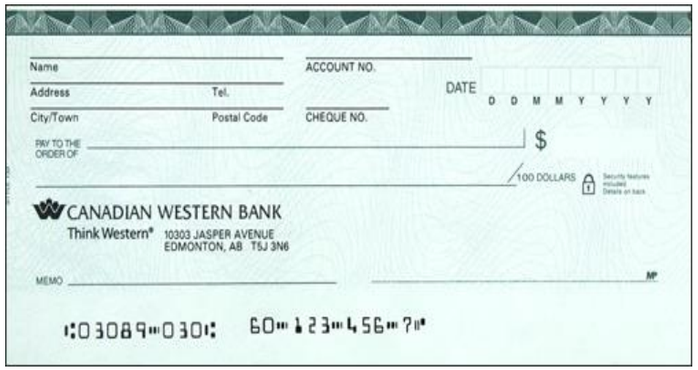
1. Finance officer for a Diocese stole over $250,000
2. The finance officer would pay church utility bills from their own personal bank account and then seek reimbursement from the church
3. The priest would routinely sign blank cheques allowing the finance officer to make cheques payable to himself

Common Causes of Church Financial Crime

- Personal use of signed blank cheques or forging of signatures
- Amending legitimate cheques
- Taking money from the offering
- Altering deposit slips
- Misappropriation of fund-raising amounts / donations etc.
- Exploiting bogus purchase orders

Financial Controls - Parishes

- Establish a finance committee
- Rotate the position of treasurer or chair every 3 years or so
- Make disbursements by cheque, draft or direct deposit
- Finance committee to regularly review bank statements
- Bank deposits should be compared over time



Financial Controls - Parishes

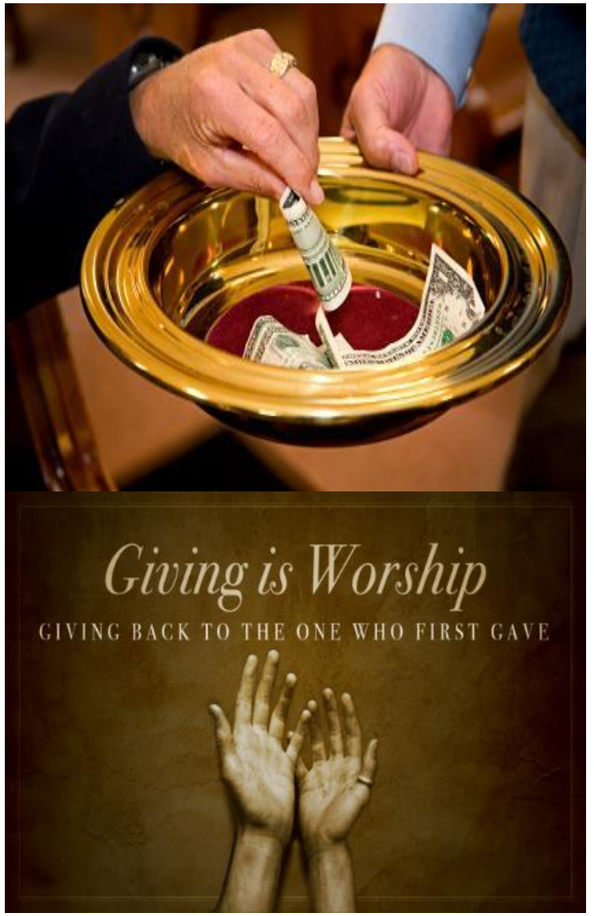
- All cheques require 2 signatures and must be fully completed before being signed
- All cheques must be supported by an invoice or purchase order
- **DO NOT SIGN BLANK CHEQUES**

Financial Controls - Parishes

- Reconcile financial records regularly
- Diocese to undertake a process of random internal audits of their Parishes finances

Offering and Tithes

- Ask worshippers to put offerings into pre-printed envelopes
- Count the offering immediately after mass in a secure area
- Use at least 2 unrelated persons to count the offering
- Rotate counting teams regularly
- Avoid counters who are experiencing financial difficulties



Offering and Tithes

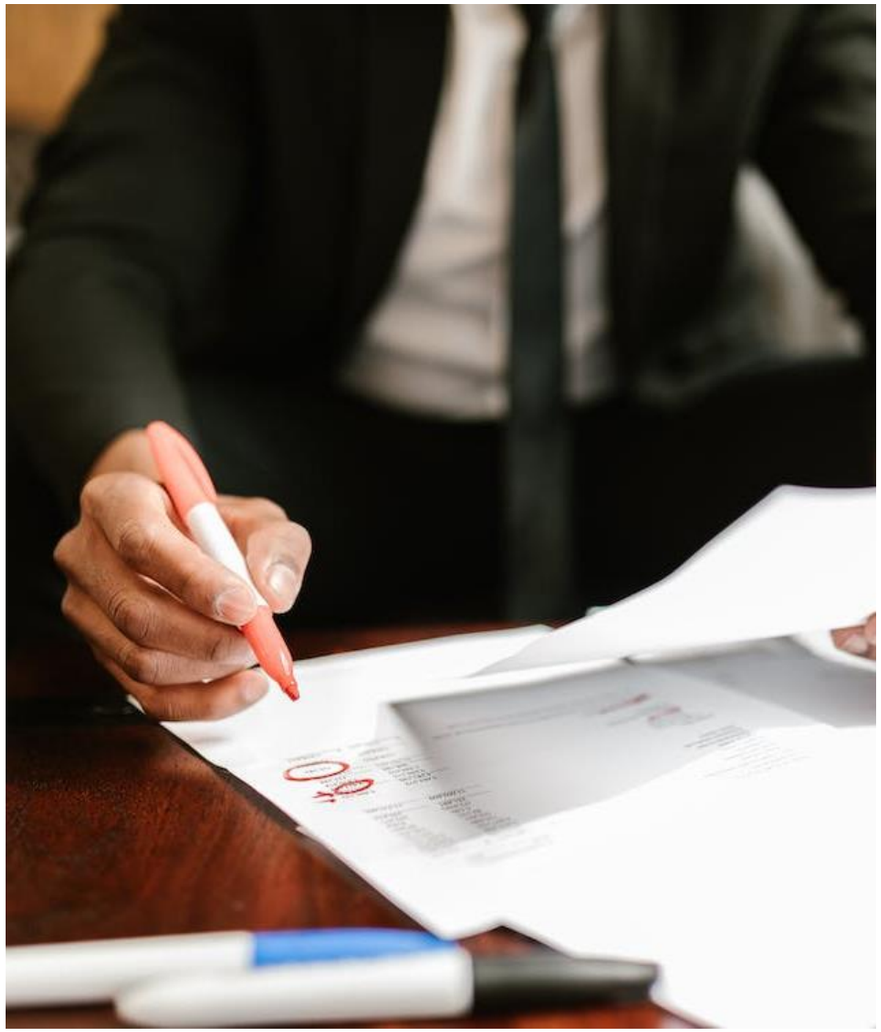
- The treasurer cannot be a counter
- Designate one counter to record the amounts received
- Ask the other to review and initial the record
- The priest or designated finance committee member should reconcile the bank account and deposit on a regular basis

Offering and Tithes

- Deposit the offering with the bank as soon as possible
- If held overnight keep money in a suitably rated safe or vault
- When making the deposit think about who should take it to the bank
- Vary times, people and routes
- Multiple trips for large deposits

Offering and Tithes

- For very large amounts use a secure cash handling service
- Compare deposits over time noting consistency or inconsistency of amounts
- Encourage members to make a direct deposit of their weekly offering and tithes



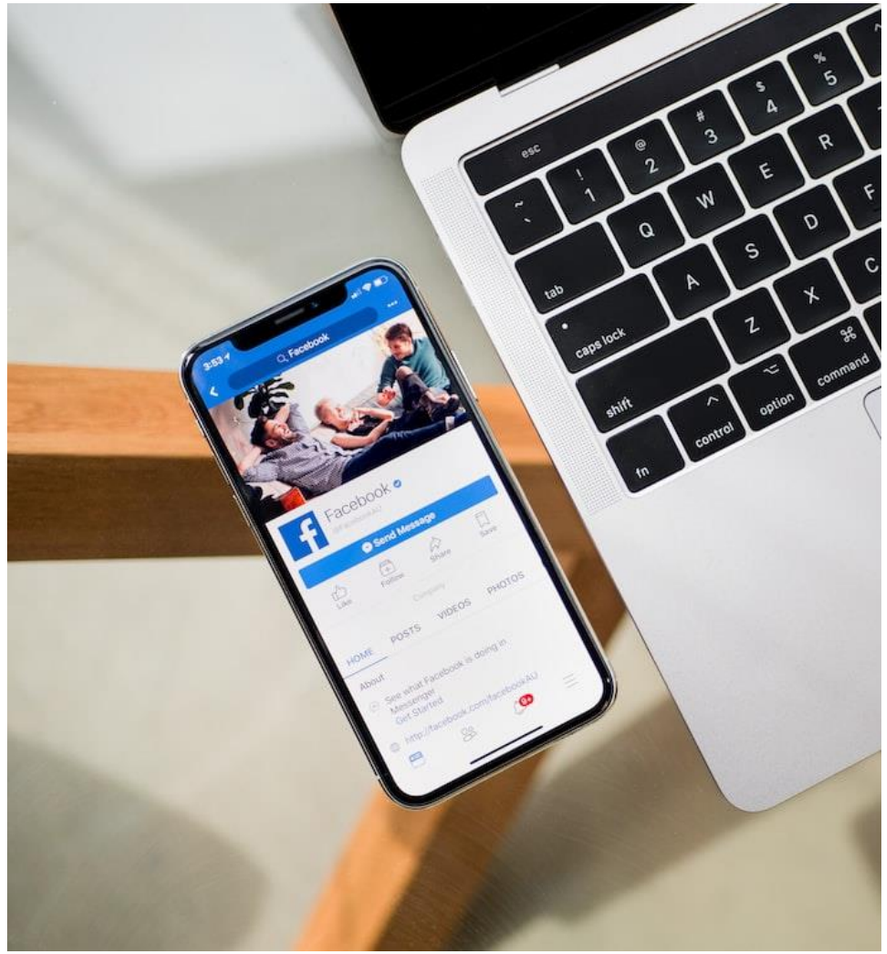
Financial Controls - Diocese

- Each diocese should have clear and comprehensive written financial policies and procedures
- Ensure the segregation of duties as far as is reasonably practical
- Maintain clear records of all financial transactions and keep these safe and secure
- Audited financial statements must be completed annually

Social Engineering Fraud

Social Engineering Fraud

- Social engineering fraud is a form of deception that exploits the human psychology rather than technical vulnerabilities to gain unauthorized access to information, funds, or resources.
- Social engineering fraud typically relies on the natural human inclination to trust and be helpful, as well as the exploitation of social norms and relationships.
- Attackers often impersonate trusted entities or individuals, such as employees, executives, or technical support personnel, to deceive their targets and gain access to sensitive information or financial assets.



Quick Quiz

Social Engineering Fraud

Common examples of social engineering fraud include:

1. **Phishing:** This involves sending fraudulent emails or messages that appear to come from reputable sources, such as banks, social media platforms, or government agencies. The aim is to trick individuals into revealing personal information like passwords, credit card details, or social security numbers.

2. **Pretexting:** In pretexting, the attacker creates a false scenario or pretense to manipulate individuals into providing sensitive information or performing certain actions. For example, an attacker may pose as a colleague or service provider to gain access to restricted areas or confidential data.

3. **Baiting:** Baiting involves enticing victims with an appealing offer, such as a free download, a gift, or a discount. The offer is used as bait to trick individuals into revealing personal information or installing malicious software on their devices.

4. **Impersonation:** Attackers may impersonate someone in authority, such as a company executive or a government official, to deceive individuals into following their instructions. This can involve requesting wire transfers, changing account details, or disclosing sensitive information.

5. **Tailgating:** In this technique, an attacker gains physical access to a restricted area by closely following an authorized person. The attacker relies on the individual's courtesy or trust to gain entry, bypassing security measures.

Preventing Social Engineering Fraud

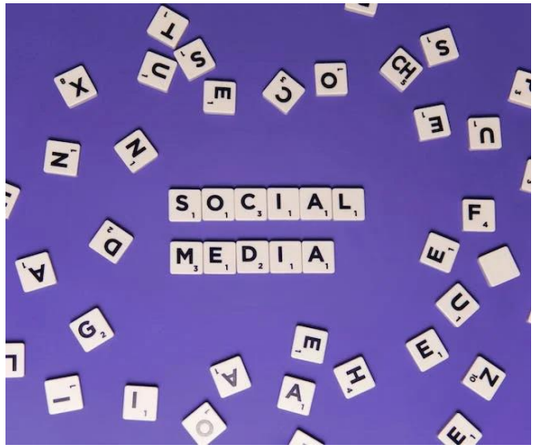
Preventing social engineering fraud requires a combination of awareness, vigilance, and security measures. Here are some important steps individuals and organizations can take to reduce the risk of falling victim to social engineering attacks:

- **Education & Awareness**: Stay as informed and up to date as possible and regularly train employees and volunteers on how to recognize and respond to social engineering threats and attempts.
- **Verify Requests and Identities**: Always verify the authenticity of requests for sensitive information or transactions, especially if they come unexpectedly or involve urgent or unusual circumstances.
- **Strengthen Password Security**: Use strong, unique passwords for all accounts and Enable two-factor authentication (2FA) whenever possible to add an extra layer of security to your accounts.
- **Be Cautious Online**: Exercise caution when clicking on links or downloading attachments from emails, messages, or unfamiliar websites.
- **Implement Security Measures**: Employ robust security software, including antivirus, anti-malware, and anti-phishing solutions, and keep them updated.
- **Physical Security:** Control access to sensitive areas and securely dispose of sensitive documents using shredders
- **Incident Reporting:** Encourage individuals to report any suspicious activity or potential social engineering attempts

PSA Trends & Litigation

PSA Trends

- **Global Impact –** frequency and severity
- **Increased Cost of Claims**
- **Social Inflation –** increased litigation & higher awards
- **Media -** #MeToo, Social Media, Mainstream press
- **Plaintiff Counsel –** New counsel handling claims
- **Class Actions –** Increase in number of Class Actions, Plaintiff-friendly courts
- **Self-Represented Litigants**



PSA Litigation

- **Loss of Income** (2019 MacLeod v Marshall)
  - Relaxed standard of proof – possible vs probable
  - Majority of Statement of Claims seek substantial damages related to loss of income
- **General Damages Cap (**Supreme Court Decision – 1979)
  - BC Court of Appeal – found that the “cap” was not applicable to sexual abuse claims
  - Now many Statement of Claims routinely claim for general damages that exceed the cap
- **Loss of Future Interdependent Relationship** (2018 K.M. v. Marson)
- **Joint & Several Liability**
  - Defendant is 1% liable, may have to pay 100% of damages
  - Impact of Mount Cashel / RCEC St. John’s
- **Coverage**
  - Duty to Defend & Uninsured Periods

Tools & Education at Your Fingertips

- **PSA Training:** https://ecclesiastical-on.safefaith.com/

Arson

Arson

Why are places of worship vulnerable to arson?

- They are targets for hate crimes
- They may attract youth fire-setters
- They may attract homeless people
- They may attract petty criminals
- Potential target for professional thieves

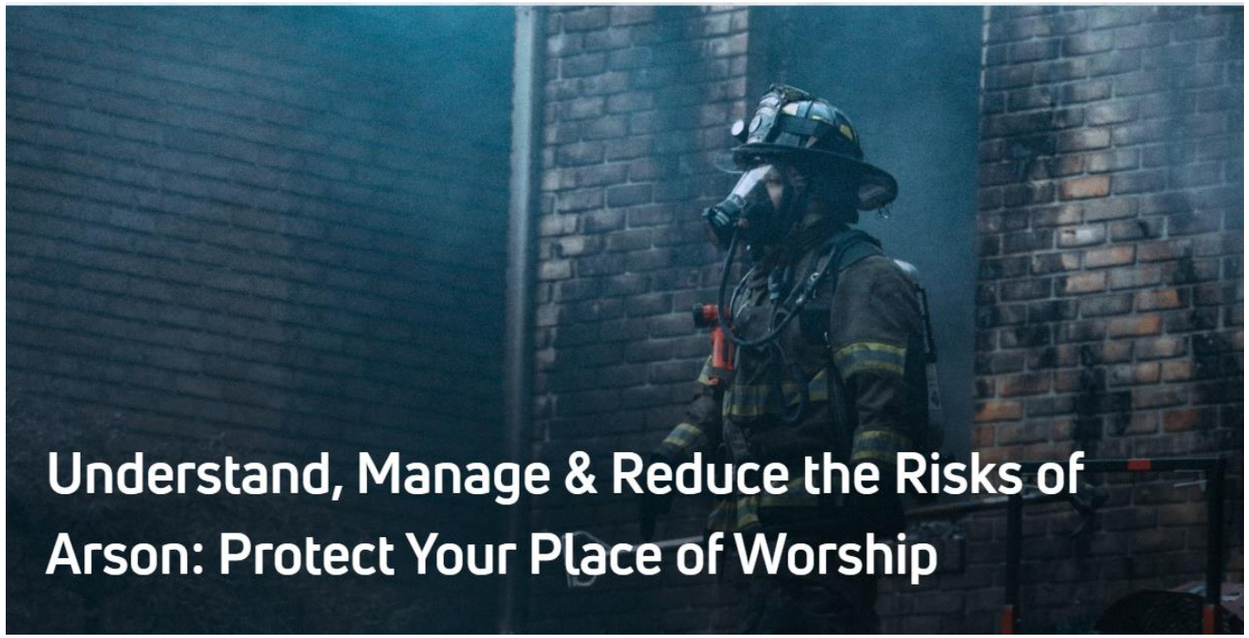
Arson

Telltale signs that a place of worship might be at risk?

- There have been small fires, break-ins or malicious damage – for example, broken windows – during the previous two years.
- There have been fires and / or break - ins in nearby places of worship in recent months.
- Groups of youths have been seen loitering near the building.
- Empty beer / liquor bottles, cigarette packages are found on the grounds.
- There is graffiti on the building.

Tools & Education at Your Fingertips

- **Risk Hub & Ecclesiastical Specialist School™:** https://ecclesiastical.ca/risk-hub/specialist-school/



Risk Management

Comprehensive Risk Management Services

- Onsite & Virtual Assessments
- Unique Property Expertise
- Risk Management Insight
- Risk Management Tools
- Replacement Cost Valuations
- Online Learning
- Conferences & Presentations
- Risk Guidance

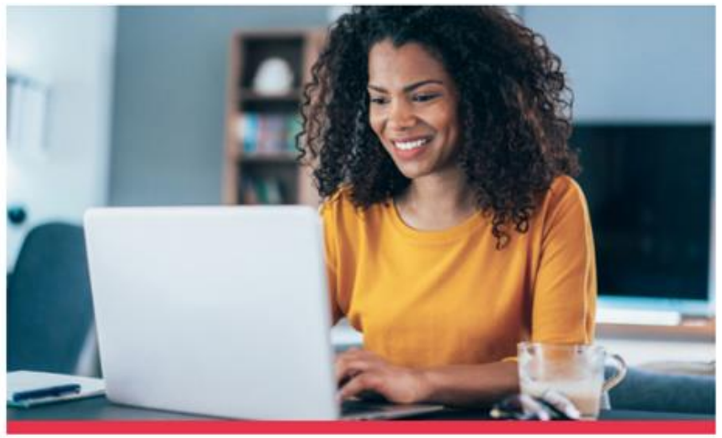
Tools & Education at Your Fingertips

- **Risk Hub**: https://ecclesiastical.ca/risk-hub/

Risk Guidance

Renowned for the risk advice and guidance we provide, the depth of our experience truly sets us apart.

Visit Risk Guidance →



Ecclesiastical Specialist School™

The Ecclesiastical Specialist School™ is an online series of courses designed to help you, your staff and your customers navigate complex scenarios with tools and best practices.

Enterprise Risk Management (ERM)

Navigating through a volatile risk landscape with Enterprise Risk Management

Tools & Education at Your Fingertips

- **Risk Guidance**: https://ecclesiastical.ca/risk-hub/risk-guidance/

Featured Resources

Windstorm Emergency Response Plan

Prepare For Winter. Protect Your property.

Are You Flood-Smart?

Tools & Education at Your Fingertips

- **Ecclesiastical Specialist School™:** https://ecclesiastical.ca/risk-hub/specialist-school/

ecclesiastical Specialist School™

Enterprise Risk Management: Managing Risks and Maximizing Opportunities

Business Continuity Planning

Best Practices on Flood Protection, Prevention & Mitigation

Slips, Trips and Falls

Arson: Protecting Places of Worship

Tools & Education at Your Fingertips

- **Enterprise Risk Management (ERM)**: https://ecclesiastical.ca/risk-hub/enterprise-risk-management/

The solution is Enterprise Risk Management (ERM)

Enterprise Risk Management is a tried and tested approach that provides organizations with a proven framework to navigate through the strategic risk landscape - successfully.

What is ERM?

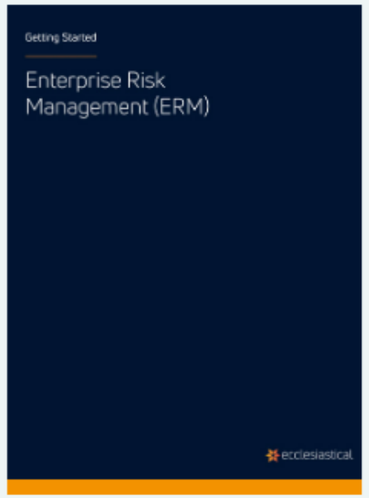
It's a process that continually identifies, assesses, manages and monitors risks across the whole organization to ensure it can make informed decisions, identify opportunities and meet their organizational objectives.

Why work with Ecclesiastical?

At Ecclesiastical we provide resources and tailored guidance to support our customers in adopting an Enterprise Risk Management approach.

Where do you start?

Take a look at our documents and templates to see how organizations can adopt an ERM approach to managing strategic risk.



Getting Started

This guide can be used as a starting point; highlighting key themes and supporting steps to help you begin your Enterprise Risk Management journey.

↓ Download

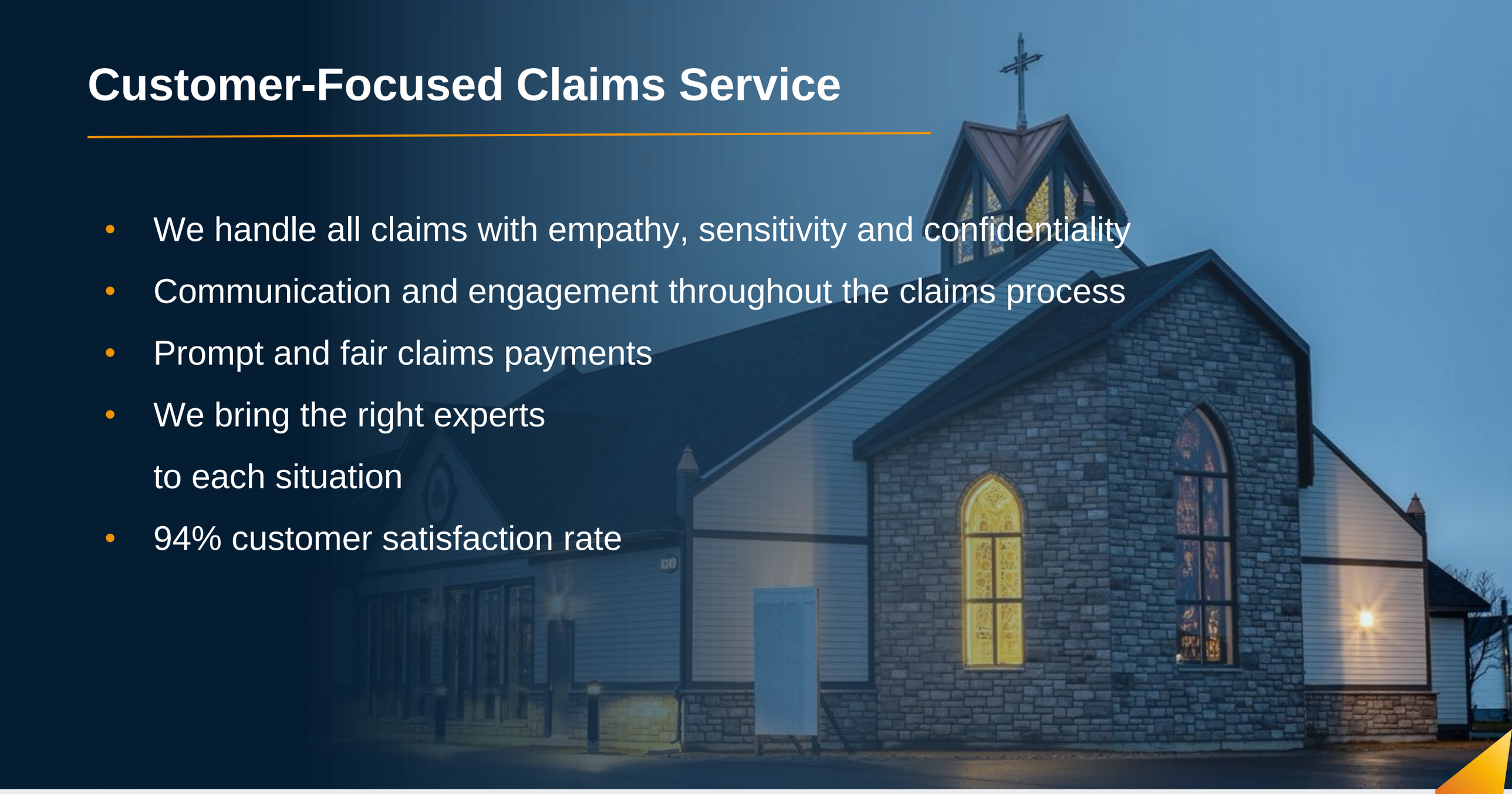
Building Inflation

Impact of Inflation

Index 2017 = 100					
Period	**Base Factor**	**Actual StatsCan Indexation**	**Adjusted Factor**	**Diocese Indexation**	**Adjusted Factor**
Q3 2017 - 2018	1.00	6.3	1.063	2.0	1.02
Q3 2018 - 2019	1.063	3.8	1.103	2.0	1.04
Q3 2019 - 2020	1.103	3.2	1.138	3.0	1.07
Q3 2020 - 2021	1.138	13.7	1.295	1.5	1.09
Q3 2021 - 2022	1.295	12.6	1.458	3.0	1.12

Offering more value

Customer-Focused Claims Service



- We handle all claims with empathy, sensitivity and confidentiality
- Communication and engagement throughout the claims process
- Prompt and fair claims payments
- We bring the right experts

  to each situation
- 94% customer satisfaction rate

Included Value-Added Services

LegalAssist

Access to experienced lawyers

ProfessionalAssist

Access to experienced
and qualified counsellors

HRAssist

Access to qualified HR
professionals and lawyers

Giving back

We are deeply involved in the community

Alzheimer Society Canada

AGA KHAN FOUNDATION

Heart&Stroke™

TIM HORTON CHILDREN'S FOUNDATION
Where kids discover their best.

UHN Princess Margaret Cancer Centre

wicc
WOMEN IN INSURANCE CANCER CRUSADE

Cystic Fibrosis Canada

THE MUSTARD SEED

YSM
YONGE STREET MISSION

SOULS HARBOUR RESCUE MISSION

NATIONAL KIDS CANCER RIDE
À VÉLO CONTRE LE CANCER CHEZ LES JEUNES

BAPS CHARITIES

bard
ON THE BEACH

EASTER SEALS DROP ZONE

SLEEPING CHILDREN AROUND THE WORLD

Kids Help Phone

The Scott Mission
A Christian Ministry of Mercy and Love

MOVEMBER

FPM
Flemingdon Park Ministry

World Vision

Giving Back

Our Community Impact Grant benefits youth, vulnerable and underrepresented people. Since 2017 the grant has awarded $2.4 million to over 200 charities.

Community Impact Grant

Thank you!