SSC # 69 – WORKING WITH VULNERABLE CLIENTS: DIGITAL TECHNOLOGY RISK MANAGEMENT

This course is eligible for:

2 Life & A&S CE Credits for BC, AB, SK, MB & ON.

General (P&C) CE Credits as marked on certificates for some Provinces.

Travel CE Credits as marked on certificates for some Provinces.

Adjusters CE Credits as marked on certificates for some Provinces.

Target Audience

This course is designed for licensed and registered financial professionals in Canada who serve individual clients across the full demographic spectrum — including aging Canadians, clients experiencing cognitive decline, and clients navigating an increasingly digital financial environment. The curriculum assumes foundational competence in client relationship management, know-your-client (KYC) obligations, and the regulatory framework governing financial services in Canada.

Primary Audience

- Licensed life and accident & sickness (A&S) insurance advisors
- General licensed advisors
- Certified Financial Planner® (CFP®) professionals and Qualified Associate Financial Planner™ (QAFP™) professionals certified by FP Canada
- Chartered Life Underwriter (CLU®), Certified Health Insurance Specialist (CHS™), and Elder Planning Counsellor (EPC) designate
- Mutual fund dealing representatives and investment dealer representatives registered with CIRO
- Financial planners and advisors operating under provincial financial planning title protection legislation (e.g., Ontario's *Financial Professionals Title Protection Act, 2019*)
- Branch managers and compliance officers responsible for supervisory oversight of client-facing advisors

Course Overview

Practice Management: Working with Vulnerable Clients and Digital Technology Risk Management is a structured continuing education course that addresses two converging practice management imperatives facing every Canadian financial advisor. The first is the growing obligation to identify, protect, and appropriately serve clients whose ability to safeguard their own financial interests is compromised — by age, cognitive decline, exploitation, or other vulnerability factors. The second is the escalating threat landscape created by digital technology — cyberattacks, data breaches, and privacy failures that can devastate both the advisor's practice and the clients it serves. These two imperatives are not separate silos. Digitally unsophisticated clients are disproportionately targeted by fraud. A firm's own cybersecurity failure can become the vector through which vulnerable clients are exploited. This course integrates both pillars into a unified practice management framework.

Learning Objectives

The following learning objectives are designed in accordance with Bloom's Revised Taxonomy, targeting the cognitive levels of application, analysis, and evaluation. Each objective is measurable through the course's 15-question summative examination and applied case studies. *Upon successful completion of this course, the learner will be able to:*

1. **Identify** the characteristics, risk factors, and observable warning signs of vulnerable clients, including cognitive decline, financial exploitation, and undue influence, within the Canadian financial advisory context.

2. **Explain** the regulatory framework governing Trusted Contact Persons (TCPs) and temporary holds under the CSA amendments to National Instrument 31-103, FP Canada Standards Council rules, and CIRO guidance.

3. **Apply** a structured response protocol when confronted with suspected financial exploitation or diminished client capacity, including documentation, internal escalation, TCP engagement, and external reporting considerations.

4. **Evaluate** the digital technology threat landscape facing Canadian financial advisory practices, including phishing, ransomware, business email compromise, and social engineering attack vectors.

5. **Distinguish** among federal and provincial privacy obligations — including PIPEDA, Quebec's Law 25, and Alberta and British Columbia PIPAs — as they apply to the collection, use, disclosure, and breach reporting of client personal information.

6. **Implement** a written incident response plan for cybersecurity events, including breach detection, containment, Real Risk of Significant Harm (RROSH) assessment, and regulatory notification procedures.

7. **Analyse** the intersection of vulnerable client protection and digital technology risk, recognising that digitally unsophisticated clients face disproportionate exposure to cyber-enabled fraud and that a firm's own security failures can become vectors for client exploitation.

8. **Design** an integrated practice management framework encompassing annual vulnerability assessments, cybersecurity reviews, staff training protocols, and policy development across both course pillars.