RISK SERVICES BULLETIN

ORGANIZATIONAL RESILIENCE PRACTICE

FRAUD ALERT: Bank Impersonation Scams Targeting Canadian Auto Dealerships

Canadian auto dealerships and businesses are being targeted by sophisticated social engineering attacks resulting in substantial financial losses. In several recent cases, dealerships have suffered multi-million-dollar losses.

The Attack Pattern:

1. **Initial Contact -** Fraudsters call the business using spoofed caller ID that displays a legitimate bank phone number, making the call appear to originate from a major Canadian financial institution

2. **Creating Urgency -** The caller claims the organization's banking system or accounts have been compromised and requires immediate action to "secure" the account

3. **Credential Harvesting -** Employees are directed to log in to what appears to be their bank's official website, but is actually a sophisticated phishing page designed to capture login credentials and multi-factor authentication (MFA) tokens

4. **Rapid Exploitation -** Using the stolen credentials and active MFA tokens, fraudsters immediately initiate multiple large electronic funds transfers (EFTs) before the fraud is detected

Why This Works: Spoofed caller ID appears legitimate, high-pressure tactics override caution, fake sites mirror real banking portals, real-time credential theft bypasses security controls, and speed limits response time.

Red Flags & Key Risk Indicators:

CALL & COMMUNICATION

- Unsolicited calls from "your bank" using high-pressure, urgent language or requests to keep the call confidential
- Requests to log in, verify access, or navigate to a specific website during the call
- Solicitation of passwords, MFA codes, or tokens - banks NEVER ask for these

TECHNICAL & WEBSITE

- Strange URLs (e.g., "rbc-secure.com" vs "rbc.com"), instructions to switch browsers, or login pages from provided links
- Certificate warnings, security alerts, unusual browser behavior, or pages requesting information in unusual sequences
- Requests to download remote access software or browser extensions

PROCEDURAL

- Instructions to bypass normal approval processes or requests for information the bank already has
- Claims of "system issues" requiring alternative login methods
- Requests for immediate large transfers or multiple failed logins blamed on technical problems

Best Practices & Protective Measures:

IMMEDIATE ACTIONS:

1. **Verify Before You Trust -** Hang up on unsolicited calls about security issues and call your bank directly using the number on your card, statements, or official website—never use caller-provided numbers
2. **Never Share Credentials -** Legitimate banks will NEVER ask you to log in during a call, request passwords and MFA codes, or direct you to a specific website to "verify" access
3. **Bookmark Official URLs** - Access banking portals only through saved bookmarks or direct URL entry—never through links in emails or calls

ORGANIZATIONAL CONTROLS TO IMPLEMENT:

- ○ **Dual Authorization -** Require two approvals for all EFTs above a specified threshold
- ○ **Transfer Limits & Delays -** Set daily limits and time delays for large or unusual transactions
- ○ **Verification Protocol -** Establish mandatory outbound callback procedures for account changes, large transfers, or security-related requests using independently sourced contact information (from prior records, not provided by the caller). Confirm new payee account details and vendor payment instructions through direct outbound calls using pre-established contact numbers before processing transfers.
- ○ **Restrict Access -** Limit employees with EFT capabilities and regularly review access lists
- ○ **Real-Time Monitoring -** Enable transaction alerts and review account activity multiple times daily
- ○ **Regular Training -** Conduct security awareness training emphasizing social engineering and banking fraud
- ○ **Incident Response Plan -** Document procedures for reporting fraud, preserving evidence, and contacting authorities

If you suspect compromise: Contact your bank immediately, change all credentials from a secure device, document everything, report to police, RCMP, and the Canadian Anti-Fraud Centre (1-888-495-8501), notify your insurer, and review all recent transactions.

How HUB Can Support You:

Cyber and crime insurance policies cover funds transfer fraud and social engineering losses but often require security controls as conditions of coverage: dual authorization, callback verification, employee training, MFA, and incident response plans. Failure to implement required protocols may limit or exclude coverage. Your HUB broker/account team stands ready to help you review the adequacy of your policies, identify required controls, ensure alignment with this bulletin's best practices, and document implementation.

The Organizational Resilience Practice within HUB's Risk Services Division provides consultative advisory services to help you prepare for and manage a wide array of fraud, cyber, and continuity risks. For resources and assistance identifying vulnerabilities and improving resilience, please engage your HUB brokerage account team.

All consulting services provided by HUB are advisory in nature. Bulletins reflect conditions observed and information supplied by clients and third-party sources and may not identify every exposure. HUB does not guarantee compliance with any law, code, or standard and does not warrant that all loss sources have been identified. Implementation of any recommendations is the responsibility of the client.