Specialty Solutions | **Social Engineering**

An organization's success depends on its employees running the day to day operations. Even the most diligent employee can be deceived into providing information to fraudsters that can result in a social engineering loss.

Social Engineering Fraud Coverage as a part of Intact's Specialty Solutions Crime Coverage insures against a variety of social engineering fraud losses including: vendors, suppliers, executives, clients and employees impersonated by a third party.

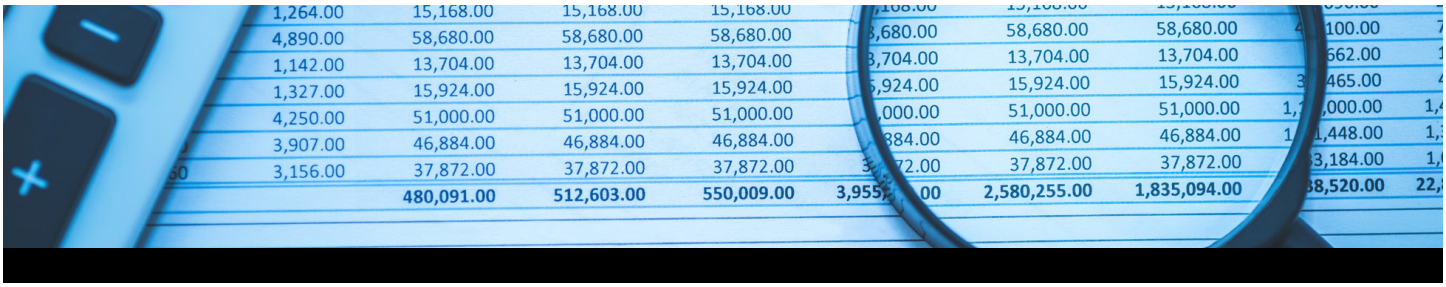
Why does an organization need social engineering coverage?

- Vendors, suppliers and clients that an organization deals with, as well as its executives and employees, can be impersonated by a fraudster requesting redirection of their next payment.
- Social engineering fraud is often not detected until the transfer of funds is completed and is discovered when the funds are not received by the authentic third party. This can cause a large financial impact to the organization.
- Social engineering fraud and scams are increasingly common and the approach is ever-changing.
- Businesses of all sizes are affected by targeted Social Engineering attacks and many of the targeted companies receive multiple attacks.

Intact Insurance Advantage

- 24/7 claims service provided by experienced examiners specializing in crime claims
- Multi-faceted accounts with crime and social engineering exposures can be placed entirely with one market
- Access to telephone-based legal and human resource services
- Superior financial stability with an A.M. Best Rating of A+
- Flexible payment options

intact INSURANCE



Coverage Highlights

Social Engineering Fraud Coverage insures a variety of social engineering fraud losses as a part of Intact's Specialty Solutions Crime Coverage, including:

- Full carve-back to the voluntary parting exclusion.
- Impersonation of vendors, suppliers, clients, executives and employees.
- Loss extends to money, securities and property.
- No call back provision within base wording.
- Broad language has no limitation on the transfer of money for loss to occur and includes communication via electronic, telegraphic, cable, teletype, telefacsimile or telephone transfer instructions.
- Coverage is provided within the crime base wording for $50,000 limit and higher limits can be purchased subject to a completed Social Engineering Supplemental Application.

Loss Examples

Require multiple sign-offs on all wire transfers:

Dual sign-offs and separation of duties can ensure you have more than one set of eyes reviewing potential fraudulent activity and can protect the company against suspicious requests.

Verify and authenticate requests:

Create company policies to ensure that all requests to transfer money require a secondary process to verify the requester. If a request is made by email, a phone call should be made by staff to the requester to ensure it was in fact their request to transfer money.

Limit company information to the public:

Company information surrounding job related duties, descriptions, out of office details and management information can help fraudsters create more convincing and specific messages to employees they wish to target.

Provide awareness and mitigation training to staff:

Provide information and training to staff on what social engineering attacks look like, how to prevent them, and what to do if they are suspicious of an interaction with a third party.

Loss Examples

Scenario One

A fraudster pretending to be an important client of a wholesaler sends in a cheque to pay the invoice for a large order. The fraudster then calls the finance team at the wholesaler and advises that the cheque was accidentally written for $20,000 more than the invoice and stresses the urgency that the finance team wire back the overpayment amount. The finance team does so; however, the cheque ends up bouncing and the wholesaler is unable to recover the $20,000 that was wired. The Crime policy indemnifies the wholesaler for the loss.

Scenario Two

An employee in the finance department of a brewery receives an email from a creditor advising that their bank account information has changed, and to forward any future payments to a new account. The email address was spoofed by a third-party, so the email appeared to be a legitimate request. The next two payments were issued to the new account prior to the brewery discovering the fraud. The loss amounted to over $1 million.

Scenario Three

An employee in the shipping department of a high-valued electronics manufacturer receives a phone call from a retailer who has an open order. The retailer advises that they would prefer the order to be shipped to their warehouse as their store location does not have space. The employee adjusts the address information on the order, and ships the product. It is later discovered that a fraudster spoofed the retailer's telephone number, and the retailer never received their order.

Contact your local underwriting team today:

British Columbia, Alberta, Saskatchewan and Manitoba:
fidelity.west@intact.net

Ontario and Atlantic Provinces:
fidelity.ontario@intact.net

Quebec:
spec@intact.net

*For more information, visit **intactspecialty.ca***

71077 (02/20)