COURT FILE NO.: CV-22-00678708-0000
DATE: 20230508

ONTARIO

SUPERIOR COURT OF JUSTICE

BETWEEN:	)	
	)	
CANASTREAM HOLDINGS LTD.	)	
	)	Aoife Quinn and Eli Lederman, for the Applicant
Applicant	)	
	)	
– and –	)	
	)	Reid Lester, for the Respondent
CHUBB INSURANCE COMPANY OF CANADA	)	
	)	
Respondent	)	
	)	
	)	
	)	**HEARD:** March 2, 2023

DINEEN J.

[1] The issue on this application is whether a cyber insurance policy covers losses suffered by a finance company for fraudulent transactions made using credit cards it had issued to customers. The charges occurred after fraudsters obtained the expiry dates and CVC codes for some of the applicant's credit card numbers through an attack on third party websites.

[2] The applicant contends that these losses fall squarely within the policy's coverage for damages arising from claims after a "cyber incident." The respondent argues that the applicant's losses were contractual payments that were expressly excluded from coverage.

[3] The applicant further takes the position that if the losses are not covered, then the doctrine of nullification of coverage should apply. It submits that these losses are the obvious risk for which it purchased this coverage and that denying recovery would be an unfair and commercially unreasonable result. The respondent submits that the policy is a liability policy that was never intended to cover the sort of property loss that the applicant suffered and that the doctrine does not apply.

[4] Finally, the applicant submits in the alternative that its loss can also be characterized as a "payment card loss" under the policy, a type of loss not covered by the contractual exclusion. The respondent submits that the definition of payment card loss does not capture what occurred here.

Factual background

The applicant's business

[5] The applicant owns a subsidiary named Fidem Finance Inc. ("Fidem") whose business model involves providing high rate, low balance credit cards to people with poor credit ratings. The cards themselves are issued by MasterCard through a license with another company, People's Trust Company ("PTC"). Fidem markets the cards and reimburses PTC for transactions made by its cardholders on a daily basis and then collects these amounts with interest from the cardholders themselves. Processing of the card transactions is performed by yet another company, Total Card Inc. ("TCI")

The insurance policy

[6] The applicant had several insurance policies with the respondent. The relevant policy is the "Cyber Enterprise Risk Management Policy" (which I will refer to as the "Cyber Policy"). The policy provides for a series of benefits for an insured including digital data recovery costs and expenses for business interruption or network extortion in the event of a ransomware or similar attack. The relevant agreement for the purposes of this application is Agreement E, the "CYBER, Privacy and Network Security Liability" agreement providing that:

> The **Insurer** will pay **Damages** and **Claim Expenses** by reason of a **Claim** first made against an **Insured** during the **Policy Period** for a **Cyber Incident** which first occurs on or after the **Retroactive Date** and prior to the end of the **Policy Period**.

[7] This agreement has a maximum $5 million policy limit. There is also coverage for "payment card loss" up to $250,000 with a deductible of $100,000.

[8] The policy contains many relevant definitions including:

> **Claim** means any: 1. written demand against any **Insured** for monetary damages or non-monetary or injunctive relief; …
>
> **Cyber Incident** means:
>
> > 1. with respect to Insuring Agreement A, Cyber Incident Response Fund, a. Any actual or reasonably suspected **Network Security Failure**; b. any actual or reasonably suspected failure by an **Insured**, or any independent contractor for whom or for which an **Insured** is legally responsible, to properly handle, manage, store, destroy, protect, use or otherwise control **Protected Information**;
> >
> > …

> 5. with respect to Insuring Agreement E, Cyber, Privacy and Network Security Liability, any error, misstatement, misleading statement, act, omission, neglect, breach of duty or other offence actually or allegedly committed or attempted by any **Insured** in their capacity as such, resulting in or based upon a **Cyber Incident** as referenced in paragraphs 1 -4 immediately above.
>
> **Damages** means compensatory damages, any award of prejudgement or post-judgement interest, **Regulatory Fines, Payment Card Loss, Consumer Redress Fund,** settlements, and amounts which an Insured becomes legally obligated to pay on account of any **Claim**. **Damages** shall not include: . . . 6. consideration owed or paid by or to an **Insured**, including any royalties, restitution, reduction, disgorgement or return of any payment, charges, or fees; or costs to correct or re-perform services, or for the reprint, recall, or removal of **Media Content**, by or on behalf of an **Insured**.
>
> **Payment Card Loss**[1] means monetary assessments, fines, penalties, chargebacks, reimbursements, and fraud recoveries, which include card reissuance costs, which an Insured becomes legally obligated to pay as a result of an Insured's actual or alleged failure:
>
> 1) of **Network Security**; or
>
> 2) to properly protect, handle, manage, store, destroy, or otherwise control **Payment Card** data, including **Protected Information**,
>
> where such amount is. . . demanded in writing from an issuing or acquiring bank that processes **Payment Card** transactions, due to an Insured's actual or alleged non-compliance with applicable **Payment Card Industry Data Security Standards**, EMV specifications, or mobile payment security requirements.

[9] The definition of "**Protected Information"** in the policy expressly includes credit card numbers.

The cyber attack

[10] The losses followed a cyber attack that began on January 2, 2020. Fraudsters targeted third party websites, apparently initially in Brazil, that allowed for online transactions where an unlimited series of combinations of invalid credit card numbers, expiration dates, and CVC

---

[1] Make sure this is the same as the endorsement modification on a61

codes could be entered without the transaction being cancelled. This allowed the fraudsters to use software to carry out a "brute force" attack by attempting different combinations until valid ones were found. The fraudsters then used the valid card information they obtained to make small trial transactions followed by large fraudulent transactions. The total fraudulent charges over the course of the subsequent four days was $1.47 million.

[11] Fidem did not become aware of the attack until January 6, when it received an email from TCI notifying it of potentially fraudulent transactions in Brazil and advising that it had blocked all Brazilian transactions two days earlier. TCI itself had received an urgent incident report on January 2 warning it of the transactions but for reasons unexplained on the record had not acted on this warning until January 4 by which time most of the fraudulent transactions had been carried out.

[12] At the end of the business day on January 6, Fidem received its daily settlement request from PTC which was far larger than expected as a result of the fraudulent charges. Fidem paid PTC as it was obliged to do according to their contractual agreement.

[13] The most detailed explanation in the record of how the fraudulent scheme succeeded is found in an incident report prepared by Fidem in January, 2020. In addition to the delay in responding to the earliest indications of the fraudulent transactions, the report explains as the cause:

> The fraudulent transactions were able to be processed on Fidem's credit cards as a result of certain fraud prevention measures not being implemented as Fidem had understood. The main issue was that transactions were presented and able to be processed as if they were chip and pin transactions when Fidem's credit cards are not chip enabled credit cards.

[14] Nothing in the record clearly identifies who should have been responsible for these fraud prevention measures being implemented or why the transactions were mistakenly processed as chip and PIN transactions.

[15] The applicant notified the respondent and made claims under a number of policies. The only one relevant to this application is the Cyber Policy. The respondent initially accepted that the losses resulted from a "Cyber Incident" as defined in the policy, but denied coverage for the bulk of the losses on the basis that they did not constitute "Damages" arising from a "Claim."

[16] The only payment made was $2500 to settle the claim of an individual cardholder who had a lawyer write a demand letter seeking compensation for inconvenience after his card was cancelled while he was on vacation as a result of the mitigation efforts made by the applicant after the fraudulent charges began.

Issues and analysis

The general principles applicable to the interpretation of an insurance policy

[17] In *Sabean v. Portage La Prairie Mutual Insurance Co* 2017 SCC 7, Karakatsanis J. summarized the analytic approach to insurance contracts as follows at para. 12:

> In *Ledcor Construction Ltd. v. Northbridge Indemnity Insurance Co*., 2016 SCC 37, [2016] 2 S.C.R. 23, this Court confirmed the principles of contract interpretation applicable to standard form insurance contracts. The overriding principle is that where the language of the disputed clause is unambiguous, reading the contract as a whole, effect should be given to that clear language: *Ledcor*, at para. 49; *Progressive Homes Ltd. v. Lombard General Insurance Co. of Canada*, 2010 SCC 33, [2010] 2 S.C.R. 245, at para. 22; *Non-Marine Underwriters, Lloyd's of London v. Scalera*, 2000 SCC 24, [2000] 1 S.C.R. 551, at para. 71. Only where the disputed language in the policy is found to be ambiguous, should general rules of contract construction be employed to resolve that ambiguity: *Ledcor,* at para. 50. Finally, if these general rules of construction fail to resolve the ambiguity, courts will construe the contract contra proferentem, and interpret coverage provisions broadly and exclusion clauses narrowly: *Ledcor*, at para. 51.

[18] Insurance contracts must be interpreted to produce reasonable results based on the commercial context in which they were negotiated. As Estey J. held for the majority in *Consolidated-Bathurst v. Mutual Boiler and Machinery Institute* (1979) 112 D.L.R. (3d0 49 (S.C.C.):

> Even apart from the doctrine of *contra proferentem* as it may be applied in the construction of contracts, the normal rules of construction lead a court to search for an interpretation which, from the whole of the contract, would appear to promote or advance the true intent of the parties at the time of entry into the contract. Consequently, literal meaning should not be applied where to do so would bring about an unrealistic result or a result which would not be contemplated in the commercial atmosphere in which the insurance was contracted. Where words may bear two constructions, the more reasonable one, that which produces a fair result, must certainly be taken as the interpretation which would promote the intention of the parties. Similarly, an interpretation which defeats the intentions of the parties and their objective in entering into the commercial transaction in the first place should be discarded in favour of an interpretation of the policy which promotes a sensible commercial result. It is trite to observe that an interpretation of an ambiguous contractual provision which would render the endeavour on the part of the insured to obtain insurance protection nugatory,

> should be avoided. Said another way, the courts should be loath to support a construction which would either enable the insurer to pocket the premium without risk or the insured to achieve a recovery which could neither be sensibly sought nor anticipated at the time of the contract.

Was this a "Cyber Incident" within the meaning of the policy?

[19] As noted above, the respondent initially accepted that a "Cyber Incident" had taken place and paid a small claim relating to a single cardholder on that basis. It has changed tack after this application was filed and now argues that that a key requirement for a finding of a Cyber Incident – a failure of network security – was not present.

[20] The applicant contends that the respondent should not be permitted to resile from its earlier acceptance that a Cyber Incident occurred. I need not decide this issue because I am satisfied that the relevant events constituted a Cyber Incident within the meaning of the contract. The definition includes a failure to properly control Protected Information, whose definition includes credit card numbers. In my view, the applicant's failure to ensure that necessary fraud prevention measures were in place to prevent the unauthorized use of the card numbers and associated expiration dates and CVC codes amounts to a failure to control Protected Information.

Was there a "claim" for "damages" within the meaning of the policy?

[21] The applicant submits that it was subject to a "claim" when PTC provided its remittance request for the daily transactions made with Fidem cards, a request that included the fraudulent charges. It notes that it had no choice but the comply with its contractual duty to make this payment and that failing to do so would have entirely undermined its relationship with PTC and its shareholders. The applicant submits that this remittance request constituted "a written demand against any Insured for monetary damages."

[22] I accept the submission of the Respondent that, irrespective of whether the PTC's remittance request would otherwise constitute a claim for damages, the exclusion for consideration in subclause 6 of the definition for damages applies. As set out above, the policy excludes:

> consideration owed or paid by or to an **Insured**, including any royalties, restitution, reduction, disgorgement or return of any payment, charges, or fees; or costs to correct or re-perform services, or for the reprint, recall, or removal of **Media Content**, by or on behalf of an **Insured**.

[23] As argued by the respondent, the payment to PTC was a purchase of receivables pursuant to the applicant's contractual relationship with PTC. This falls squarely within the definition of "consideration."

[24] The applicant submits that the term "consideration" is ambiguous and that the ambiguity in an exclusion must be resolved against the insurer. It submits that "consideration" could

also be reasonably interpreted to mean only consideration offered for the formation of new contracts and not payments made pursuant to pre-existing contracts like its contract with PTC.

[25] I disagree that it is logical to read the policy as drawing such a distinction and do not see the term as ambiguous. I am reinforced in that conclusion by the fact that the policy would also have excluded PTC's claim in damages had the applicant declined to make the required payment. Exclusion 11 of the policy provides that :

> The **Insurer** shall not be liable for **Costs, Damages**, or **Claims Expenses** on account of any **Incident** or any **Claim**…
>
> > for breach of any express, implied, actual or constructive contract, warranty, guarantee, or promise, including any actual or alleged liability assumed by an **Insured**, unless such liability would have attached to the **Insured** even in the absence of such contract, warranty, guarantee, or promise. However, this exclusion shall not apply to:
> >
> > a. solely with respect to Insuring Agreement E, **Payment Card Loss**;,
> >
> > b. an **Insured's** contractual obligation to maintain the confidentiality or security of Protected Information;

[26] The policy read as a whole in my view clearly excludes the sort of business loss suffered by the applicant, which it distinguishes from other sorts of legal liability for damages suffered by others due to the exposure or loss of private information from a cyber attack on the policy holder.

Were the losses suffered by the applicant "Payment Card Loss"?

[27] I do find, however, that the losses suffered by the applicant are captured by the definition of "Payment Card Loss" in the policy. The policy provides that the contractual exclusion does not apply to Payment Card Loss. I find that the demand for payment from PTC for fraudulent card charges that it processed falls within the range of payments covered in the definition which include "monetary assessments," "reimbursements," and "fraud recoveries."

[28] The respondent submits that the Payment Card Loss claim fails because there is no evidence that the loss resulted from "actual or alleged non-compliance with applicable **Payment Card Industry Data Security Standards**, EMV specifications, or mobile payment security requirements." It is true that the evidence in the record about the exact nature of the security failure that led to the loss is lacking in detail. Nonetheless, in my view it is an irresistible inference that a failure to implement fraud prevention protocols permitting credit card transactions to erroneously present as chip and PIN transactions

would necessarily amount to non-compliance with the requisite security requirements, and that the applicant is ultimately responsible for this.

Does the doctrine of nullification of coverage apply?

[29] In the event that the policy is found not to cover its losses or to cover only $150,000 as payment card loss, the applicant submits that the doctrine of nullification of coverage should be applied. It submits that the loss it suffered was, given its business model, obviously the very sort of loss that motivated it to take out the policy in question for which it paid substantial premiums. To interpret the policy to provide no or minimal recovery in the face of a cyber attack causing losses from fraudulent transactions on its customers' credit cards would, in the applicant's submission, be to deny it the benefit of the coverage that it was paying for. It relies on the statement of Rosenberg J.A. at para. 28 of *Cabell v. The Personal Insurance Company* 2011 ONCA 105:

> If the court is able to determine on an objective basis that the insurer's interpretation would render nugatory coverage for the most obvious risks for which the endorsement is issued, a tactical burden shifts to the insurer. It will be for the insurer to show that the effect of its interpretation would not virtually nullify the coverage and would not be contrary to the reasonable expectations of the ordinary person as to the coverage purchased.

[30] I disagree. This is not, in my view, a situation comparable to the authorities relied on by the applicant, such as *Weston Ornamental Ironworks Ltd. v. Continental Insurance Co.,* [1981] O.J. No. 78 (C.A.) where a restrictive reading of a policy substantially negated coverage for an individual policy-holder leaving the company pocketing the premiums without risk.

[31] While the coverage provided for payment card loss may be relatively low, it is not the case that the applicant received no potential benefit from the "CYBER, Privacy and Network Security Liability" coverage given its type of business. The policy would cover the applicant in the event of a ransomware attack or a hack of the applicant's computer systems resulting in the loss of customer personal information and consequent legal liability. I cannot say on the record that the applicant was not at any real risk of significant liability from such an attack.

[32] On my reading of the policy, that type of attack is the obvious risk at which it is directed and is what the reasonable person taking out this insurance would understand was covered. To the extent that the applicant was motivated to buy the policy to protect against a different type of loss, I do not agree that the doctrine of nullification of coverage enables me to enforce its expectations against the respondent. I cannot say on the record before me that it was clearly commercially unreasonable for the applicant to pay for the policy on the interpretation that I have found or that it creates an unrealistic or unfair result.

Disposition

[33] The application is allowed in part and the applicant is awarded judgment in the amount of $150,000. If the parties are unable to settle the issue of costs, the applicant may submit brief costs submissions within two weeks of the date of this judgment and the respondent will have two further weeks to respond.

Dineen J.

Released: May 8, 2023

COURT FILE NO.: CV-22-00678708-0000
DATE: 20230508

ONTARIO

SUPERIOR COURT OF JUSTICE

BETWEEN:

CANASTREAM HOLDINGS LTD.

Applicant

– and –

CHUBB INSURANCE COMPANY OF CANADA

Respondent

REASONS FOR JUDGMENT

Dineen J.

Released: May 8, 2023