Court of King's Bench of Alberta

Citation: Serinus Energy PLC v SysGen Solutions Group Ltd, 2023 ABKB 625

Date: 20231107
Docket: 2001 07294
Registry: Calgary

Between:

Serinus Energy PLC

Plaintiff/
Defendant by Counterclaim

- and -

SysGen Solutions Group Ltd.

Defendant/
Plaintiff by Counterclaim

Reasons for Judgment
of the
Honourable Justice M.A. Marion

Table of Contents

I. Introduction

[1] At its core, this case addresses a simple question: can a commercial IT service provider, without notice and under the guise of protecting the client's information systems, reset a client or former client's administrator account passwords to gain leverage in a billing dispute when there is no contractual, statutory or other claimed common law right to do so? The answer is no.

[2] Does the answer change if the client is difficult or the client's position in the billing dispute is incorrect? No: the answer is still no.

[3] People and businesses rely increasingly on complex electronic information systems to manage their information. Most do not have the technical skills or resources to protect themselves from cyberthreats or manage their own IT systems. They often need help from professionals with technical experience and special skills. Absent clear and enforceable contractual language, statutory rights, or other common law rights, it would never be reasonably expected that IT professionals hired and authorized to manage and protect information systems would use their privileged access to disrupt their client or former client's business for the IT professional's benefit in a billing dispute. Such conduct would be a marked departure from ordinary standards of decent behaviour.

[4] In this case, the Defendant, SysGen Solutions Group Ltd (**SysGen**), was not attempting to steal from its client, the Plaintiff, Serinus Energy PLC (**Serinus**), or to damage Serinus' IT systems. However, SysGen used its continued access to Serinus' information systems to remove Serinus' administrator access to Serinus' own systems at a time when Serinus (to the knowledge of SysGen) was transitioning away from SysGen to a new IT services provider. SysGen changed Serinus' administrator passwords which locked Serinus out from administrative control of its systems, without notice to Serinus and immediately after Serinus disputed a SysGen invoice for services during the transition period. SysGen asserts that it did this to investigate or monitor a security threat to Serinus' systems. When SysGen failed to return administrator access, and instead made a settlement offer using Serinus' administrator access as part of a settlement of the billing dispute, Serinus took matters into its own hands and managed to break into its own systems to regain control.

[5] This summary trial raises issues about the proper interpretation of the parties' contract, including an amendment to the contract and its termination provisions. It also raises the questions of whether SysGen breached the contract, committed the tort of conversion, breached fiduciary duties, and whether the tort of intrusion upon exclusion should be recognized in this case. Further, SysGen disputes Serinus' damages, including the reasonableness of its response and expenses incurred. Serinus also claims aggravated and punitive damages, which SysGen asserts are excluded by a contractual exclusion clause. Finally, SysGen counterclaims against Serinus for unpaid invoices during and after the transition period, which Serinus has refused to pay.

[6] For the reasons set out below, I find that SysGen breached the contract between the parties and committed the tort of conversion. However, SysGen did not owe fiduciary obligations, and this is not an appropriate case to consider whether the tort of intrusion upon seclusion can or should be recognized in Alberta. SysGen is liable for some of Serinus' costs in response to SysGen's conduct, and for punitive damages which are not barred by the contractual exclusion clause. However, Serinus is also liable to SysGen for some of SysGen's unpaid invoices for services Serinus received and used.

[7] The net result of this litigation, after set-off, is a judgment in favour of Serinus against SysGen in the amount of $43,874.61 plus pre-judgment interest from June 1, 2020 to the date of this judgment, and post-judgment interest to the date of payment, at the prescribed rate under the *Judgment Interest Act*, RSA 2000, c J-1.

II. Procedural Background

[8] Serinus filed its Statement of Claim on June 9, 2020. Serinus claims that SysGen infiltrated Serinus' IT systems and performed an unauthorized password reset on all of Serinus' administrator accounts, intentionally blocking Serinus from managing or overseeing its own IT infrastructure, with the intent to ransom Serinus for disputed SysGen invoices. Serinus claims breach of contract, breach of fiduciary duty, conversion, and intrusion upon seclusion. It claims general damages, aggravated damages, and punitive or exemplary damages.

[9] On June 16, 2020, SysGen filed a claim against Serinus in the Provincial Court of Alberta (as it was then known), claiming $53,000 plus interest for goods and services provided pursuant to contracts alleged between Serinus and SysGen.

[10] On September 9, 2020, Master Mason (as she then was) ordered the transfer of SysGen's Provincial Court action to the Court of Queen's Bench (as it then was) and its consolidation with Serinus' claims in this action.

[11] On October 27, 2020, SysGen filed its Statement of Defence and an Amended Counterclaim which, among other things, amended the Counterclaim to $58,118 and added a claim of unjust enrichment.

[12] On November 9, 2020, the parties consented to the terms of a procedural Consent Order. They then engaged in a process involving the filing of numerous affidavits and conducted several questionings on affidavits, working toward the summary trial that was held on March 2 and 3, 2023.

III. The Record

[13] The parties relied exclusively on a 1,455-page jointly-filed Compendium of Pleadings & Evidence (**Compendium**), which includes evidence from 13 witnesses.

[14] Serinus' witnesses were:

(a) Jeffrey Auld (**Auld**), Serinus' CEO, by way of an affidavit and questioning pursuant to rule 6.7;

(b) Moez Mansouri (**Mansouri**), Serinus' Head of IT, by way of two affidavits and questioning pursuant to rule 6.7;

(c) Rhonda Yaniw (**Yaniw**), Serinus' Head of Corporate Administration, by way of two affidavits and questioning pursuant to rule 6.7; and

(d) Stephen Mathezer (**Mathezer**) of iON United Inc (**iON**), by way of an expert report and questioning thereon.

[15] SysGen's witnesses were:

(a) Lyle Richardet (**Richardet**), SysGen's CEO, by way of three affidavits and questioning pursuant to rule 6.7;

(b) Shane Jordan (**Jordan**), SysGen's Director of Service Delivery, by way of three affidavits and questioning pursuant to rule 6.7;

(c) Jordan Charuk, SysGen's Client Experience Specialist, by way of two affidavits. He was not questioned on his affidavits;

(d) Matthew Mowser (**Mowser**), SysGen's Technical Account Representative, by way of two affidavits and questioning pursuant to rule 6.7;

(e) Ryan Pentlichuk, (**Pentlichuk**), SysGen's Virtual IT Manager, by way of one affidavit upon which he was not questioned;

(f) Michael Swallow (**Swallow**), SysGen's Manager of Client Services, by way of two affidavits and questioning pursuant to rule 6.7;

(g) Ryan Stock (**Stock**), SysGen's Field Service Manager, by way of two affidavits upon which he was not questioned;

(h) Sanad Rustom (**Rustom**), SysGen's Technical Account Representative, by way of three affidavits and questioning pursuant to rule 6.7; and

(i) Christopher Kayser (**Kayser**) of Cybercrime Analytics Inc, by way of two expert reports and questioning thereon.

[16] The parties agreed that the evidence in the Compendium, other than the expert reports which were objected to pursuant to rule 5.36, was admissible evidence subject only to the weight that the court might place on that evidence.

[17] The record before the court was significant. No *viva voce* evidence was heard or requested and the matter proceeded directly to two days of final argument. By my estimation, with the significant record the parties condensed what would likely have been a two-week trial into two days of argument. It was, in effect, a "trial in a box".

IV. Factual Background

[18] The material factual background in this matter is largely undisputed. A summary of the factual background is set out below, which is based on what appears to be agreed or undisputed evidence, or my factual findings.

A. The Parties and their Business Relationship

[19] Serinus is a publicly-traded international oil and gas company with active operations and offices in Romania and Tunisia, together with offices in Calgary and London. SysGen is an IT services provider with its head office in Calgary.

[20] The parties' relationship started in 2010. In May 2010, Serinus (under a previous name) applied for an account with SysGen by executing an Account Application (**2010 Application**). The parties disagree as to whether the 2010 Application ever became legally binding on the parties, was in effect at the times relevant in this action, and about its legal effect.

B. The FSMA, the Standard Set-Up and Other Services

[21] The parties agree that, in December 2015, they entered into a contract called a Field Service Maintenance Agreement (**FSMA**). Pursuant to the FSMA, SysGen agreed, for a $11,000 monthly fee, to provide services related to the management of Serinus' IT systems (**FSMA Services**), including: (1) continuous monitoring; (2) asset management services; (3) maintenance of the security of Serinus' IT environment without introducing new security risks; (4) holding quarterly business reviews in respect of Serinus' IT systems; and (5) maintaining the confidence of Serinus' internal structure and its marketing strategies. The monthly fee included a guarantee that SysGen would provide an on-site person at Serinus' Calgary offices on a full-time basis (**On-Site FTE**). The FSMA excluded a number of other IT services from its scope.

[22] It is acknowledged by both parties that, at all relevant times, Serinus owned its IT systems, including its servers. However, the FSMA did not expressly provide how administrator access to Serinus' IT systems would be handled. The experts agree that there were several potential IT service model structures available to provide the FSMA Services. SysGen's preferred practice was to have sole global administrator access over its client's IT systems, which meant that only SysGen would be able to make changes to the IT systems where administrator access was required. Accordingly, until January 2020, SysGen was set up as the sole privileged holder of global administrator access over the Serinus IT system (referred to by SysGen as the **Standard Set-Up**). The Standard Set-Up was in place until end of January 2020.

[23] In addition to the FSMA Services, SysGen provided Serinus other services. In December 2016, November 2017, and May 2018, the parties agreed to the terms of purchase orders by which SysGen provided Serinus with data backup drives and ongoing storage services (**Data Storage Services**). Further, in July 2018, the parties agreed to the terms of a purchase order by which SysGen would provide Serinus with licences to Office 365 software (**Software Licence Services**).

C. The Relationship Strains and Amendment to the FSMA

[24] By June 2019, Serinus had concerns with SysGen's On-Site FTE, Mowser, who had been the On-Site FTE since 2013. At a June 2019 quarterly business review (**QBR**) meeting, the parties discussed replacing him. SysGen agreed to take immediate steps to remove Mowser and to work with Serinus to provide different support. By June 2019, Mowser was no longer on-site and the parties implemented a new support structure involving on-site support in the morning and remote support in the afternoon.

[25] The parties explored whether a new FSMA arrangement could be put into place. In July, 2019, SysGen proposed a new FSMA with a lower monthly fee of $9,000 and a two-year term. It was not acceptable to Serinus, in part because Serinus was not in a position to enter into a new commitment on a two-year term. Serinus advised that the parties would have to revert back to the existing arrangement.

[26] On August 20 and 21, 2019, by email exchange, the parties agreed to amend the FSMA (**FSMA Amendment**), the legal effect of which is in dispute. In summary, Serinus takes the position that the FSMA was amended to reduce the monthly fee to $9,000, to replace the On-Site FTE with on-site support in the mornings and remote support in the afternoons, and to convert the FSMA to a contract with a month-to-month term. SysGen agrees with Serinus' position regarding

the monthly fee but says that the amendment did not change the provisions of the FSMA dealing with its term or termination.

[27] Following the FSMA Amendment, SysGen invoiced and Serinus paid $9,000 per month and Serinus no longer received the equivalent of the On-Site FTE.

[28] In fall 2019 and early 2020, the relationship between the parties continued to be somewhat strained, particularly in respect of Auld's dealings with SysGen and his dissatisfaction with SysGen's services.

D. Serinus Requests and Receives Administrator Access to Serinus' Systems

[29] In January 2020, Mansouri was appointed Serinus' Head of IT with the mandate of managing and supervising Serinus' IT infrastructure. Mansouri wanted Serinus to have administrator access to its own systems (**Administrator Access**) to reduce risks in the event a problem arose that required immediate administrator access. The Standard Set-Up was no longer acceptable and he requested SysGen provide him Administrator Access.

[30] SysGen initially refused to provide Mansouri with Administrator Access. On January 29, 2020, SysGen (Jordan) met with Serinus (Auld) to explain SysGen's intent to maintain the Standard Set-Up, and provided Serinus a letter indicating that it could not provide Mansouri Administrator Access as long as the Serinus infrastructure is SysGen's responsibility.

[31] Serinus responded by demanding that Mansouri be provided Administrator Access by January 30, 2020, failing which Serinus would consider the FSMA to have been terminated with cause. SysGen relented and provided Mansouri with Administrator Access. When it did so, it stated: "Please note SysGen is no longer responsible for the environment or if anything breaks now that we have provided access to another party". Serinus replied: "You have provided access to you [sic] client. Your responsibilities remain intact".

E. SysGen's Termination of the FSMA

[32] Deviating from the Standard Set-Up was not acceptable to SysGen due to its concerns over liability. Accordingly, on January 31, 2020, SysGen wrote to Serinus to terminate the FSMA (**Termination Letter**). The Termination Letter provided (emphasis in original):

> Effective today, January 31, 2020, SysGen are here by providing notice of termination of our Managed Services Contract with Serinus Energy. Per the agreed to contract terms, SysGen are providing 90 days' notice of termination of services. Effective May 1, 2020, SysGen will no longer provide on-site/off-site Managed Service Support with the exceptions below:
>
> **1) Microsoft Office Licensing [...]**
>
> **2) SysGen Back-up and Business Continuity Service [...]**
>
> **As part of this 90 day notice period**:

1) SysGen agrees to work with Serinus Energy to transition services in an expeditious and professional manner.

2) SysGen has already provided administrator access and passwords to Serinus IT personnel.

3) Should any disruption of services be caused by any Serinus internal IT personnel or third parties, SysGen will not be held liable.

4) If SysGen is required to remedy any issues outside of our normal FSMA agreement these hours will be billed back to Serinus Energy at a time and materials rate of $160 paid in advance to SysGen before work will commence.

5) We respectfully ask that all and any outstanding amounts are paid to SysGen prior to May 1, 2020.

[...]

[33] Serinus did not respond to the Termination Letter.

[34] Following the Termination Letter, SysGen's services were primarily related to the transition of services. However, SysGen continued to provide some FSMA Services, Data Storage Services and Software Licence Services in February, March and April 2020. For example, Serinus continued to make service requests to SysGen, SysGen continued to log into accounts on the Serinus system, SysGen continued to provide at least some regular recurring managed service (or "service level agreement" events as outlined in the FSMA), and SysGen continued to provide reports that it had normally provided under the FSMA. SysGen continued to provide on-site services until at least mid March 2020, although the FSMA Services related to on-site and remote support were reduced after February 2020. During this period, Serinus paid at least one invoice in respect of the FSMA Services.

[35] There is a dispute about the effect of the Termination Letter and SysGen's entitlement to be paid for the various services after it was sent.

F. Serinus Retains IT Ops and Shuts Down Office Due to COVID

[36] Following the Termination Letter, SysGen did not provide a formal transition plan. Mansouri began more actively managing Serinus' IT systems. By mid-February, Yaniw had directed Serinus staff to send their IT requests to Mansouri, although, as noted above, some IT service requests continued to be made to SysGen. In early March 2020, Serinus repeated its request for an inventory of all Serinus software licenses and access logins for those licences, which Serinus needed as part of the transition of services.

[37] By early March, as part of the transition away from SysGen's services, Serinus did several other things, including: (1) resetting passwords; (2) installing its own monitoring software (**Site 24x7**); (3) installing a cloud-based application (**Altera**) to allow Mansouri to remotely access Serinus computers; (4) retaining a Calgary-based IT services company, IT Ops, to assist with the

management of Serinus' Calgary server and to replace some of the FSMA Services previously provided by SysGen; and (5) providing IT Ops with Administrator Access.

[38] Serinus took at least some of these steps without consulting with or giving notice to SysGen. However, by March 4, 2020, SysGen employees, including Rustom, Stock and Jordan, became aware of some of Serinus' transition steps including that Serinus had been making "backdoor administrator level changes" to Serinus' systems, and that Serinus had retained a new IT services provider to which Serinus had provided Administrator Access. In fact, in early March, Rustom met with Serinus and IT Ops' representative, James Idris (**Idris**), in respect of the transition of services. At that time, Jordan, as SysGen's Director of Service Delivery, did not see Serinus' transition steps as a security threat. SysGen did not advise Serinus that those steps were problematic and did not take any immediate steps in response to secure Serinus' IT environment or remove Serinus' or IT Ops' Administrator Access.

[39] By March 15, 2020, when Serinus shut its Calgary office down due to COVID, Serinus had provided written notice to SysGen that IT Ops was its new IT service provider and that IT Ops may wish to work with SysGen as part of the transition of services from SysGen to IT Ops.

[40] During March 2020, SysGen continued to provide transition services and at least some FSMA Services, including remote support and some on-site support until March 15, 2020 when Serinus shut its offices down.

G. Serinus Requests Removal of SysGen's RMM Software

[41] On April 2, 2020, Serinus requested that SysGen remove SysGen's remote monitoring and management software (**RMM Software**), known as "LabTech", from Serinus' systems. The RMM Software was required by SysGen to remotely access Serinus' system and was a step consistent with the transition of services away from SysGen. In response to the request, SysGen confirmed that its RMM Software was being automatically removed from any Serinus online machines and would take several hours. However, SysGen did not remove all the RMM Software. It retained the ability to remotely access Serinus' system.

H. The Disputed Invoice and the Administrator Lockdown

[42] By a letter dated April 20, 2020, but sent by email in the early morning of April 21, 2020, Serinus wrote to SysGen (**Dispute Letter**) to dispute (**Billing Dispute**) Invoice ADV-39769, notwithstanding Serinus had paid the invoice almost a month earlier.

[43] In the Dispute Letter, Serinus disputed the legal effect of the Termination Letter with SysGen for the first time. Serinus took the position that the Termination Letter was a letter of resignation effective January 30, 2020 and that SysGen had invalidly attempted to create a 90-day notice period upon its resignation. Serinus requested SysGen to provide the contractual basis upon which SysGen was entitled to continue to be paid its fees.

[44] On April 20 or 21, 2020, Jordan advised SysGen's CEO, Richardet, about surreptitious third-party access and changes to Serinus' IT systems. Richardet instructed SysGen's Manager of Client Services, Swallow, to return Serinus' system to the Standard Set-Up, so that SysGen was

the sole privileged holder of global administrator access over Serinus' IT system (**Administrator Lockdown**).

[45] Using, at least in part, the SysGen's LabTech RMM Software that Serinus had requested SysGen remove, Swallow implemented the Administrator Lockdown at approximately 10:06 am on April 21, 2020 by resetting certain passwords. Following the Administrator Lockdown, certain Serinus accounts were disabled, Serinus and IT Ops no longer had Administrator Access to Serinus' Calgary IT server (and in particular its domain controller), Mansouri and Idris had lost their email access entirely, and Serinus access to SQL service accounts used for a Serinus geological project database were disabled. As Mansouri deposed: "Serinus could not maintain, change, manage or have any visibility into the functioning of its own IT systems". Serinus could not continue to transition its services to its new IT provider. It only had end-user access.

[46] SysGen did not seek or obtain Serinus' specific authorization to implement the Administrator Lockdown. It provided no advance notice to Serinus.

I. Response to the Administrator Lockdown and the Billing Dispute

[47] On April 21, 2020, within a few hours of the Administrator Lockdown, Serinus realized it no longer had Administrator Access and that Swallow was remotely accessing its system. Serinus advised SysGen that it had lost Administrator Access, and asked SysGen for information about why that had happened and who Swallow was. SysGen confirmed Swallow was a SysGen employee, that SysGen "would have a response for you soon," and that they were "investigating and working on it". SysGen did not advise Serinus that SysGen had completed the Administrator Lockdown, or why Serinus had lost its Administrator Access, even though SysGen knew these things.

[48] Using its own Altera RMM Software, Serinus managed to access and observe its Calgary server and to get the logs for the account responsible for the Administrator Lockdown (an account named "Waterboy"). In the very early hours of April 22, 2020, Serinus emailed the password logs to SysGen, asked SysGen whether a SysGen computer had been infected with malware, and requested more information about the Waterboy account and what was going on. Serinus advised SysGen it was a "very high level security issue for our infrastructure".

[49] SysGen never responded to Serinus' email. However, after Serinus sent SysGen this email, SysGen uninstalled Serinus' Site 24x7, Altera and other remote access software. With its own RMM software uninstalled, Serinus could no longer remotely access its own systems and could not provide IT support to Serinus staff. However, with Administrator Access, SysGen continued to have access to all of Serinus' data and information on Serinus' Calgary server. At that point, Serinus for the first time believed that SysGen was deliberately denying Serinus Administrator Access. Mansouri notified Serinus' CEO, Auld.

[50] Later on April 22, 2020, SysGen responded to Serinus' Dispute Letter. SysGen's response asserted its right to be paid for the disputed invoice and future invoices for its services since the Termination Letter. SysGen's response did not mention the Administrator Lockdown or provide Serinus any information about it.

[51] On April 23, 2020, Serinus responded to SysGen about the Billing Dispute, but also stated:

> Finally, I would draw your attention to a deeply concerning incident that occurred on 22 April 2020.[1] At approximately 10:00 am MDT we registered and retained logs on an unidentified device accessing our active domain server. This device had access with high level administration account credentials and whilst in the system changed all the domain administration passwords. Please investigate and confirm that this unauthorized device was not undertaken by, or with the knowledge of, SysGen, its employees or associates. If any such person was involved, we request that any revised passwords be provided to us immediately so that we may regain fully [sic] access Serinus' IT assets and systems. Your written confirmation is required immediately.

[52] SysGen did not respond.

[53] On April 24, 2020, Serinus' counsel wrote to SysGen, asserted that SysGen was hijacking Serinus' systems, and demanded that SysGen immediately return Administrator Access to Serinus by 6 pm that day, failing which Serinus "will be taking steps to restore its access including through the Courts without further notice to you". In the meantime, Serinus began taking preparatory steps to regain access and had shut down its servers by late afternoon on April 24.

[54] SysGen responded immediately to the April 24, 2020 letter. However, it did not return Administrator Access to Serinus. Instead, it sent an offer through its legal counsel, the full contents of which are not in evidence.

[55] SysGen had not restored Administrator Access by the 6 pm deadline. Serinus' CEO instructed Mansouri to do whatever it took to restore Serinus' control of its IT systems.

[56] Serinus worked with IT Ops over the weekend and, by April 26, 2020, using a forced administrator password reset with a server boot disk, had restored Serinus' control over all the administrator accounts on its Calgary server (**Serinus Restoration**). There is a dispute between the experts as to the appropriate characterization and reasonableness of what Serinus did to regain control of its IT systems. SysGen's position is that the Serinus Restoration was a reckless self-help measure.

[57] After the Serinus Restoration, SysGen no longer had access to Serinus' Calgary server.

[58] On April 27, 2020, Serinus retained iON to perform a cyber incident investigation with a view to securing Serinus' environment from any further unauthorized access and ensuring there were no "time bombs" or further threats in the system. Serinus relied on input from iON and Mansouri in authorizing the iON work (**iON Work**), which included creation of a May 19, 2020 report.

[59] In its Stament of Defence, SysGen asserted that the Administrator Lockdown was the continuation of the FSMA Services during the 90 day notice period, and was a response to a security threat in the Serinus system.

[1] Based on the evidence, I find that this date is in error and should have April 21, 2020.

V. Issues

[60] The issues in this summary trial application are:

(a) Is this an appropriate matter for summary trial?

(b) Are the expert opinions admissible?

(c) Is SysGen liable to Serinus for breach of contract?

(d) Is SysGen liable for conversion?

(e) Is SysGen liable for breach of fiduciary duty?

(f) Is SysGen liable for the tort of intrusion upon seclusion?

(g) If SysGen is liable to Serinus, what are its damages, including:

(i) What are Serinus' compensatory damages?

(ii) Is this an appropriate case for punitive damages?

(h) Is Serinus liable to SysGen on the Counterclaim?

(i) If Serinus is liable to SysGen, what are SysGen's damages?

VI. Analysis

A. Is this an Appropriate Matter for Summary Trial?

[61] Part 7, Division 3 of the *Alberta Rules of Court*, Alta Reg 124/2010 (*Rules*) governs summary trials.

[62] The well-established and binding test for whether a summary trial is appropriate is twofold: (1) can the court decide disputed questions of fact on affidavits or by other proceedings authorized by the *Rules* for a summary trial? and (2) would it be unjust to decide the issues in such a way? See: ***JN v Kozens***, 2004 ABCA 394 at para 40; ***Imperial Oil v Flatiron Constructors Canada Limited***, 2017 ABCA 102 at para 24; ***SHN Grundstuecksverwaltungsgesellschaft MBH & Co v Hanne***, 2014 ABCA 168 at para 9. This test must be viewed through the lens of proportionality: ***Benke v Loblaw Companies Limited***, 2022 ABQB 461 at para 16.

[63] Whether the first part of the twofold test will be met will depend on the nature and quality of the material before the court: ***Compton Petroleum Corp v Alberta Power Ltd***, 1999 ABQB 42 at para 20. Perfect evidence is not required. The evidence need only be sufficient to permit the judge to find the facts necessary to adjudicate the issues of fact or law and reach a just result: ***956126 Alberta Ltd v JMS Alberta Co Ltd***, 2020 ABQB 718 at para 225, citing ***Beaver First Nation Band v Bulldog***, 2004 ABCA 79 at para 5; ***Goulbourne v Buoy***, 2003 ABQB 409 at para 26. Further, conflicting evidence is not alone a bar to summary trial if the conflict can be resolved by reference to other evidence, or if the disputed evidence is immaterial: ***571582 Alberta Ltd v NV***

Reykdal & Associates Ltd, 2000 ABCA 330 at paras 2–4 ; ***Jagodnik v Oudshoorn***, 2015 ABQB 456 at para 5; ***WestJet v ELS Marketing Inc***, 2013 ABQB 666 at para 63, rev'd in part 2014 ABCA 299; ***Benke*** at paras 13–19; ***Compton*** at para 20.

[64] In this case, the parties have done an excellent job and spent significant resources marshalling and organizing the evidence of numerous witnesses, several of whom have been questioned on their affidavits. There is an extensive documentary record. Both parties agree that there are not significant disputes in the evidence as to "what happened", but rather disputes about the legal effect of things that happened. Both parties agree that a trial judge would not likely obtain any further or better evidence than that presently before the court.

[65] With respect to the second part of the test, for many years Alberta courts have frequently referred to a non-exhaustive list of factors to consider whether it would be unjust to proceed by summary trial: ***Schaufert v Calgary Co-Operative Association Limited***, 2021 ABQB 579 at para 4; ***Jagodnik*** at para 3; ***Factors Western Inc v DCR Inc***, 2019 ABQB 971 at para 35; ***HOOPP Realty Inc v Guarantee Company of North America***, 2018 ABQB 634 at para 17; ***O'Neil v Yaskowich***, 2018 ABQB 599 at para 12; ***Duff v Oshust***, 2005 ABQB 117 at para 24; ***Compton*** at para 21; ***Adams v Norcen Energy Resources Ltd***, 1999 CanLII 19063 (ABQB), 248 AR 120 at para 19.

[66] Those factors are:

(a) the amount involved;

(b) the complexity of the matter;

(c) its urgency;

(d) any prejudice likely to arise by reason of delay;

(e) the cost of taking the case forward to a conventional trial in relation to the amount involved;

(f) the course of the proceedings;

(g) whether all witnesses or only some were (will be) cross-examined in court;

(h) whether there is a real possibility that the defendant can bolster its evidence by discovery of the plaintiff's documents and witnesses; and

(i) whether the resolution will depend on findings of credibility.

[67] I would add to this list: whether the parties agree that a summary trial is appropriate. The Court of Appeal has warned courts that we should not give unreasonable weight to the agreement of the parties as to the suitability of the summary trial process, and should not pre-judge the analysis based on party agreement before the other factors are considered: ***Imperial Oil*** at paras 44–46. I interpret this only to mean that the parties' agreement is not determinative but is one factor to consider. In my view, an agreement of summary trial suitability is an important factor because it respects that counsel will have the best understanding of the issues at play, because it

provides public access to justice for matters that may not financially justify a full trial process or to parties that may not be able to afford private dispute resolution, and because it, in turn, supports the rule of law. See: ***Hannam v Medicine Hat School District No 76***, 2020 ABCA 343 at para 48; ***Benke*** at para 7.

[68] Courts must also consider the existence of credibility issues in context. "Credibility" issues include both issues of credibility (sincerity or willingness to speak the truth as the witness believes it be) and reliability (accuracy of an honest witness' evidence): ***R v Delmas***, 2020 ABCA 152 at para 25, citing ***R v Morrisey***, 1995 CanLII 3498 (ONCA), 22 OR (3d) 514. One of the factors a court can consider in assessing credibility is to observe demeanour, which might include responsiveness, fairness, and objectivity versus evasiveness, exaggeration and partisanship: ***557466 Alberta Ltd v McPherson***, 2022 ABQB 23 at para 112. While first-hand observation of demeanour is preferable, some aspects of demeanour can be assessed (albeit imperfectly or at times with more difficulty) through review of a questioning transcript and other records.

[69] Further, Courts of Appeal have cautioned against over-reliance on demeanour because it may have limited value: ***R v Giroux***, 2017 ABCA 270 at para 7; ***R v Rhayel***, 2015 ONCA 377 at para 85. Other non-exclusive and overlapping factors in assessing credibility include (a) the plausibility of the evidence; (b) independent supporting or contradicting evidence; (c) the external consistency of the evidence; (d) the internal consistency of the evidence; and (e) the balance of the evidence: ***R v Harris***, 2022 ABKB 759 at para 19, citing Justice David M. Paciocco, "Doubt about Doubt: Coping with *R. v. W(D.)* and Credibility Assessment" (2017) 22 Can Crim L Rev 31 at 65. And, further, courts may use the reason and common sense, life experience and logic provided they do not fall into prejudicial or stereotypical reasoning: ***Delmas*** at para 31; ***R v ARD***, 2017 ABCA 237, aff'd ***R v ARJD***, 2018 SCC 6; ***Harris*** at para 20. First-hand observation of live witnesses is often important to resolve credibility, but in some civil cases will not be necessary or a proportionate process.

[70] In my view, courts should be reluctant to refuse to hear a matter by way of summary trial too readily only because of credibility issues. This is particularly so where the parties agree that summary trial is appropriate, knowing full well the contents of the record and any conflicts or credibility issues arising in the evidence.

[71] Whether credibility can be fairly determined in a transcript-and-records-based summary trial will be directly correlated to the robustness of the record. The more well-prepared and concise the affidavits, the more those affidavits are tested by questioning, and the more objective documentary or other evidence there is available, the more likely the court can resolve credibility without having to observe the witnesses first-hand. In those circumstances, courts should give the evidence a hard look before refusing summary trials in favour of a full trial process.

[72] On the other hand, where parties provide affidavits that are unsupported, untested or questioned upon, or that make bald assertions or conclusory statements, vague references, personal opinions, or hearsay, it will be more difficult for the court to proceed where there are conflicts or credibility issues. If parties expect a summary determination, they must ensure there is an appropriate record.

[73] In this case, the amounts at issue are relatively small. The matter is reasonably complex but not unduly so. The parties have expended significant resources preparing affidavits; and

conducting numerous questionings on affidavits, to put a robust record before the court. It is doubtful that much more additional evidence would be garnered through an expensive and delayed trial process. There are some credibility issues, the key one being whether SysGen's evidence of the reason it initiated the Administrator Lockdown is honest or reliable evidence. Both parties agreed the matter is appropriate for summary trial. I am satisfied, having completed my detailed review of the evidence, that there is sufficient evidence for me to make fact findings, to resolve any credibility issues, and that it would be just to resolve this dispute on the record before me. I do not require *viva voce* evidence in this matter.

B. Are the Expert Opinions Admissible?

[74] Each party relies on an expert report. The experts were extensively questioned before trial. The reports and the questioning transcripts were included in the Compendium. Several factual witnesses swore affidavits directly responding to the expert evidence. As a matter of efficiency, the parties agreed that, rather than making a preliminary ruling on admissibility of the expert reports during the summary trial, I would decide admissibility and weight to be given to the reports after trial as part of my deliberations.

[75] The admission of expert evidence remains a two-step process. At the first step, the proponent of the evidence must establish the threshold requirements of admissibility, which are the four ***Mohan*** factors from ***R v Mohan***, 1994 CanLII 80 (SCC), [1994] 2 SCR 9 at 20, namely relevance, necessity in assisting the trier of fact, absence of any exclusionary rule, and a properly qualified expert: ***White Burgess Langille Inman v Abbott and Haliburton Co***, 2015 SCC 23 at para 23; ***R v Bingley***, 2017 SCC 12 at para 14.

[76] It is within the properly qualified expert component of the analysis that the court considers the expert's duty to the court to be fair, objective and non-partisan, and their willingness and capacity to comply with it: ***White Burgess*** at para 53. The expert's opinion must be impartial (reflecting an objective assessment of the questions at hand), independent (it is the product of the expert's independent judgment, uninfluenced by who has retained them or the outcome of the litigation) and unbiased (it does not unfairly favour one party's position over another): ***White Burgess*** at para 32.

[77] If the evidence does not meet the threshold ***Mohan*** requirements, it should not be admitted: ***Bingley*** at para 15. As summarized in ***Bingley*** at para 15:

> If at the first stage, the evidence does not meet the threshold *Mohan* requirements, it should not be admitted. The evidence must be logically relevant to a fact in issue: *R. v. Abbey*, 2009 ONCA 624, 97 O.R. (3d) 330, at para. 82; *R. v. J.-L.J.*, 2000 SCC 51, [2000] 2 S.C.R. 600, at para. 47. It must be necessary "to enable the trier of fact to appreciate the matters in issue" by providing information outside of the experience and knowledge of the trier of fact: *Mohan*, at p. 23; *R. v. D.D.*, 2000 SCC 43, [2000] 2 S.C.R. 275, at para. 57. Opinion evidence that otherwise meets the *Mohan* requirements will be inadmissible if another exclusionary rule applies: *Mohan*, at p. 25. The opinion evidence must be given by a witness with special knowledge or expertise: *Mohan*, at p. 25. In the case of an opinion that is based on a novel scientific theory or technique, a basic threshold of reliability of the

> underlying science must also be established: *White Burgess*, at para. 23; *Mohan*, at p. 25.

[78] At the second discretionary gatekeeping step, the court balances the potential risks and benefits of admitting the evidence in order to decide whether the potential benefits justify the risks and benefits or potential harm to the trial process: ***White Burgess*** at para 24; ***Bingley*** at para 16. Those risks, benefits or harm can include prejudice, consumption of time, or confusion: ***White Burgess*** at para 24. If the probative value is outweighed by its prejudicial effect, it should be excluded: ***Mohan*** at 21; ***White Burgess*** at paras 19, 24; ***Bingley*** at para 16.

[79] I consider the proposed expert evidence below under this framework.

1. Kayser

[80] SysGen relies on Kayser's primary and surrebuttal expert reports. It seeks to have him qualified as an expert in the area of cybersecurity in information technology administration. Kayser was not involved in the underlying events in this action.

[81] In his report, Kayser answered six questions, but they really surrounded three main topics. Question 1 dealt with whether the Standard Set-Up, and SysGen's efforts to maintain the Standard Set-Up, was consistent with industry standards. Questions 2-5 addressed what Kayser defined as a "brute force attack" (or **BFA**) to regain access to an IT system, including the risks involved, when a BFA would be a reasonable step to take, what sort of qualifications a person should have before using a BFA, and the potential costs if the risks of using a BFA were realized. Question 6 addressed whether a cybersecurity incident response would be necessary or reasonable once administrator control was restored.

[82] I find that the questions as presented are logically relevant to issues in the action, namely whether the Administrator Lockdown was in accordance with industry standards, and whether the Serinus Restoration and other steps taken by Serinus in response to the Administrator Lockdown were reasonable in the circumstances (which is relevant to damages). I am also satisfied that the expert opinion is necessary in the sense that it will assist me in appreciating these matters in issue. There are no exclusionary rules that would preclude its admission.

[83] I have some concerns about Kayser's qualifications given his lengthy work history, which, until 2016, was focussed on now-outdated computer programming, sales, management and investment advisory work, not cybersecurity or IT. Further, I am satisfied that, based on his most recent work experience and education over the past number of years, and in particular his Master of Criminal Justice and Graduate Certificate in Cybercrime Investigation and Cybersecurity from Boston University, he is sufficiently and properly qualified to give opinions in the area of cybersecurity. Limitations on his qualifications are better addressed in this case as a matter of weight to be given those opinions. Further, I find he is not qualified to give opinion evidence on technical aspects of information technology administration, IT managed services, or IT support services.

[84] Kayser's evidence goes into some details that are tangential at best, and in my view in some areas he spent an inordinate amount of time going down some paths that were not overly helpful to the Court. In oral argument, SysGen's counsel acknowledged that the evidence respecting the

BFA was probably not as relevant as it may have originally seemed. Had I not had the benefit of the questioning already being conducted, and I was determining whether to admit all aspects of his report in the first instance at a trial, I would have found that the benefits of Kayser's evidence (at least in some areas) was outweighed by the risks to the trial, particularly in relative time consumption and expense. However, I have had to review the questioning transcripts in any event, and limited additional time was spent at trial on the expert evidence. On balance, in these unique circumstances, I find that the benefit of the admissible evidence outweighs its risks or prejudicial effects.

[85] However, even if qualified as an expert, external independent witnesses must limit their testimony to their area of expertise: ***R v McPhail***, 2019 ABCA 427 at para 4, citing ***R v Sekhon***, 2014 SCC 15 at para 46. Embedded in Kayser's report and questioning testimony are opinions he is not qualified to make, in particular legal opinions about what Serinus or SysGen were "entitled" to do or not do, and interpreting the FSMA or the FSMA Amendment. That evidence is not admitted and is ignored. Further, I do not admit or rely upon any opinions he gives in the technical aspects of information technology administration, IT managed services, or IT support services.

[86] Further, at times Kayser was argumentative and in my view strayed into advocacy, for example in his steadfast attempt to interpret the contractual entitlements of the parties. This did not reach the level of requiring all of his evidence to be inadmissible as contemplated in ***White Burgess***, but it did affect the weight I gave his evidence.

2. Mathezer

[87] Serinus relies on Mathezer's expert report and testimony. Unlike Kayser, Mathezer was involved in the events in the underlying litigation. Serinus retained his firm to conduct the iON Work on April 27, 2020. Mathezer's report responds to Kayser's report and the six questions, and in doing so also explains what iON did and found as part of the iON Work following the Administrator Lockdown and the Serinus Restoration.

[88] Because he was involved in the underlying events in this matter, Mathezer is a different kind of "witness with expertise" than Kayser. In ***Kon Construction Ltd v Terranova Developments Ltd***, 2015 ABCA 249 at para 35, the Court of Appeal noted that there are at least three categories of "witnesses with expertise":

> (a) Independent experts who are retained to provide opinions about issues in the litigation, but were not otherwise involved in the underlying events. This is the category of expert witness contemplated by ***White Burgess*** and ***Mohan***.
>
> (b) Witnesses with expertise who were involved in the events underlying the litigation, but are not themselves litigants. An example is the family physician in a personal injury case who is called upon to testify about his or her observations of the plaintiff, and the treatment provided.
>
> (c) Litigants (including the officers and employees of corporate litigants) who have expertise, and who were actually involved in the events underlying the litigation. [...]

[89] Mathezer fits into the second category of witness with expertise. In ***Kon Construction*** at para 37, the Court of Appeal suggested that it is prudent to qualify witnesses in the second category much like independent experts who were not involved in the underlying events:

> [37] It is sometimes argued that the evidence of witnesses in the second category is not "opinion" evidence: ***Westerhof*** at paras. 60-1. To some extent they are testifying about what they observed, and what they actually did. In that sense, they are not opinion witnesses. On the other hand, it is challenging for them to explain why they acted as they did without engaging their professional expertise. For example, the family doctor cannot explain why he or she endorsed any particular treatment without expressing a medical opinion about it. It is difficult to set the boundary between what they did and their expert opinions about what should have been done. **Where witnesses with expertise (who are not litigants) are to testify about events within the scope of their expertise, it is generally prudent to have them formally qualified as expert witnesses, particularly when they propose to express opinions on collateral issues like the employment prospects of the patient.** Further, the overall objective of comprehensive disclosure found in R. 5.1(1)(c & d) supports the pre-trial disclosure of the opinions of participating experts. [Emphasis added]

[90] In responding to Kayser's report, Mathezer purports to express opinions beyond his direct involvement, and I find it is prudent to go through the two-step process for qualifying him as an expert witness and admitting his report.

[91] Mathezer's evidence is relevant and necessary, for the same reasons outlined earlier for Kayser's evidence. Further, embedded in Mathezer's evidence is also evidence about what exactly he and iON observed when they were working for Serinus, which is relevant evidence that includes factual evidence. There are no exclusionary rules that would preclude admission of Mathezer's evidence.

[92] With respect to whether Mathezer is a properly qualified expert, Serinus did not clarify the area in which they sought to have Mathezer qualified as an expert. SysGen does not dispute he is an expert in respect of general IT principles. Based on his education (including his Bachelor of Computer Science), training and experience, I also find he has expertise in cybersecurity assessment and the design, implementation, support and management of cybersecurity solutions. I am satisfied, that with respect to Questions 1-5, Mathezer is a properly qualified expert and exhibited impartiality, independence and a lack of bias. The fact Mathezer was retained by Serinus is not enough to undermine his independence, impartiality and freedom from bias: ***White Burgess*** at para 32.

[93] However, I find Mathezer's evidence in respect to Question 6 should not be admitted. The evidence discloses that Serinus retained Mathezer and iON to assist with the incident response. As part of that, Mathezer and iON advised Serinus about the recommended next steps once Serinus had regained Administrator Access and control of its IT systems. The question of whether the iON Work was necessary and reasonable in the circumstances effectively puts Mathezer's advice directly in issue. Mathezer acknowledged that an adverse finding about the reasonableness of the response could affect iON's reputation. I find that there is a realistic concern that Mathezer, while perhaps willing, is unable to provide independent and unbiased expert opinion evidence on the

question of whether the iON Work was a necessary and reasonable response. Therefore, Serinus has not discharged its burden to establish threshold admissibility of that evidence. Accordingly, "those parts" of his evidence are excluded: ***White Burgess*** at para 48. However, this does not render all his evidence inadmissible, including his evidence in respect of Questions 1-5.

[94] Further, as a factual witness with expertise, Mathezer's evidence about why he and iON recommended particular steps, and to explain what they did, is admissible. His observations are admissible as factual evidence: ***Kon Construction*** at paras 35–37.

[95] For the same reasons as with respect to Kayser, I am satisfied that the benefits of Mathezer's evidence (other than his opinion evidence specifically related to whether the iON Work was necessary or reasonable in Question 6) outweighs the risks to the trial or any prejudicial effect.

[96] Like Kayser, Mathezer also ventured into legal opinions based on his interpretation of the contractual or other entitlements of the parties. He also referenced and interpreted the *Criminal Code*, RSC 1985, c C-46. As with Kayser, Mathezer's legal opinions are not admitted and will be ignored.

[97] Further, I have given less or no weight to certain of Mathezer's opinions which were based upon incorrect assumptions. For example, Mathezer was advised (incorrectly) that SysGen had resigned and was no longer authorized to be accessing Serinus' IT systems as of January 2020.

3. Employees of the Parties with Expertise

[98] Neither party objected to the evidence of the other party's employee witnesses who at the time arguably provided opinion evidence based on their expertise. For example, employee witnesses on both sides have expertise in IT systems (for example, Mansouri for Serinus; and Rustom, Mowser, Pentlichuk and Swallow for SysGen). Given the lack of objection and the principles set out ***Kon Construction*** at paras 35(c) and paras 38–43, any such opinions within their expertise that they gave in the context of explaining what they did and why, were admissible and I considered them in the context of all the evidence.

C. Is SysGen Liable for Breach of Contract?

[99] Although its written argument focused more heavily on its tort and fiduciary duty claims, Serinus' Statement of Claim pleads breach of contract. Contractual issues in this action include whether the 2010 Application was a binding legal contract that continued to bind the parties in 2020, and the interpretation of the FSMA after the FSMA Amendment (to determine the contractual obligations of the parties at the time of and following the Termination Letter and between the Termination Letter and the Administrator Lockdown).

1. Was the 2010 Application a Contract Binding on the Parties?

[100] SysGen argues that the 2010 Application became a binding legal agreement between the parties that was still applicable in 2020. It relies on the 2010 Application primarily in relation to its Counterclaim, which is addressed later in these Reasons.

[101] Serinus argues that the 2010 Application was only signed by Serinus as an application or an offer, that SysGen did not sign it, and that there is insufficient evidence of its acceptance by SysGen. It relies on the principle that an acceptance of an offer must be communicated to the offeror before acceptance is complete and a binding contract is created: ***Schiller v Fisher***, [1981] 1 SCR 593, 1981 CarswellOnt 523 at para 8. Serinus asserts that the 2010 Application is a "foisted unilateral agreement" that does not bind Serinus, relying on: ***Meads v Meads***, 2012 ABQB 571; ***John W Page Welding Consulting Ltd v Canonbie Contracting Limited***, 2014 ABQB 465 at para 48; ***Park Place Communities Ltd v Wong***, 2017 ABQB 725 at para 11.

[102] I disagree with Serinus' characterization of the 2010 Application. I find that the 2010 Application was executed and agreed to by Serinus and returned to SysGen. SysGen's provisions of the blank application to Serinus to fill out was the offer — SysGen offered to provide services if Serinus accepted the terms of the 2010 Application. The execution of the 2010 Application was Serinus' acceptance. This is clear based on Serinus' signature line on the 2010 Application, which stated: "the undersigned below warrants the above information is true, and agrees to the Terms and Conditions on the reverse. **Accepted** this 12 day of May 2010" (emphasis added). The consideration was that SysGen agreed to provide future services to Serinus based on those Terms and Conditions.

[103] Serinus points to one aspect of the language in the attached Terms and Conditions (relating to credit) as evidence that the filled-out 2010 Application was the "offer" by Serinus to SysGen. That part of the Terms and Conditions provided that Serinus understood that "if our Organization is approved for credit, we will be subject to the terms as specified by SysGen...". In my view, this does not make the 2010 Application an offer. It simply provides that, under the 2010 Application agreement, SysGen may accept Serinus for credit and, if that happened, then Serinus agreed to the credit terms. This conditional credit provision was only one part of the agreement — the 2010 Application agreement also dealt with non-solicitation, third party software indemnity, and limitation of liability, all of which would be applicable even if Serinus was not accepted for credit.

[104] Even if I am wrong in my characterization, there is evidence that SysGen and Serinus worked together for approximately ten years, and that SysGen provided services and invoiced for those services. If necessary, I would find on the balance of probabilities that, by its conduct, SysGen accepted Serinus' offer reflected in the 2010 Application.

[105] Accordingly, I find on the balance of probabilities that the 2010 Application was a contract governing the business relationship between Serinus and SysGen. As there is no evidence it was ever terminated, I find that it continued to be an active contract between them as of 2020, including at the time of the Termination Letter and the Administrator Lockdown.

2. The FSMA Amendment

[106] The parties dispute the proper interpretation of the FSMA Amendment and, in particular, whether it only reduced the price and services under the FSMA, or also amended its term and termination provisions.

[107] The goal of contractual interpretation is to determine the objective intent of the parties at the time the contract was made through the application of legal principles of interpretation: ***IFP Technologies (Canada) Inc v EnCana Midstream and Marketing***, 2017 ABCA 157 at para 79;

Sattva Capital Corp v Creston Moly Corp, 2014 SCC 53 at para 49. Contracts must be interpreted in light of the contract as a whole: ***IFP*** at para 79; ***Tercon Contractors Ltd v British Columbia (Transportation and Highways)***, 2010 SCC 4 at para 64.

[108] In interpreting contracts, courts must consider the relevant surrounding circumstances, including the objective evidence of the background facts at the time of execution of the contract, namely the knowledge that was or reasonably ought to have been within the knowledge of both parties at or before the date of contracting: ***IFP*** at paras 82–83; ***Sattva*** at para 58. Relevant background facts can include the genesis, aim or purpose of the contract, the nature of the relationship created by the contract, the nature or custom in the industry in which the contract was executed, antecedent agreements leading up to the contract, and even negotiations if they shed light on the factual matrix: ***IFP*** at paras 83–85 and the cases cited therein; ***Alberta Union of Provincial Employees v Alberta Health Services***, 2020 ABCA 4 at para 32.

[109] Surrounding circumstances does not include the parties' subjective intentions, and surrounding circumstances cannot be used to add to, detract from, vary or otherwise overwhelm the written words: ***Sattva*** at paras 59–60; ***IFP*** at paras 81–82; ***Alberta Union*** at para 26.

[110] If the terms of an agreement are ambiguous, then the court may refer to extrinsic evidence, including the parties' post-contractual conduct, to resolve the ambiguity: ***IFP*** at paras 86–87; ***Shewchuk v Blackmont Capital Inc***, 2016 ONCA 912 at paras 46, 56. Mere difficulty in interpreting a contract is not the same thing as ambiguity; a contract is ambiguous when the words are reasonably susceptible to more than one meaning: ***IFP*** at para 86.

[111] The surrounding circumstances relevant to the interpretation of the FSMA Amendment include the following:

(a) the parties had been operating under the FSMA for over three years;

(b) the FSMA had been automatically renewed effective in January 2019 for a term ending January 2020;

(c) the On-Site FTE that had been used for quite some time had been removed and was no longer providing on-site services as of approximately June 2019;

(d) on July 2, 2019, SysGen proposed an updated arrangement in the form of a new Master Services Agreement for a two year term. Serinus advised SysGen that it was not in a position to enter into a new commitment for two years and, therefore: "for now we will just revert back to our existing arrangement";

(e) at an August 2019 QBR meeting, the parties met to discuss possible changes to the FSMA. Serinus again confirmed it was unwilling to commit to a one or two year term on a proposed agreement. The parties discussed the fact that Serinus continued to pay the FSMA's $11,000 monthly charge even though SysGen had not provided the "guaranteed" On-Site FTE under the FSMA for July and August; and

(f) at that August 20, 2019 QBR meeting, there was an agreement to continue with the setup where there would be on-site IT support in the morning and remote services in the afternoon, with a reduced price of $9,000 per month.

[112] The FSMA Amendment was then crystallized in a few emails, the pertinent portions of which are set out below:

> *Serinus to SysGen*: Per our conversation last week, the outcome of the meeting was that Serinus could not commit to a one or two year term on the proposed Service Agreement therefore we would need to continue under the terms and conditions of the existing Service Agreement from 2016 where the monthly cost is $11,000 per month which includes a guaranteed full-time resource. Can you tell me when that schedule will start? We have been without an onsite full-time resource basically for the month of July and August but still paying the $11,000 / month.
>
> *SysGen to Serinus*: I have been meaning to get back to you as I have some great news. I have been really pushing back with our President about signing a new contract right now and in light of the long term relationship and trying to do what's best for Serinus as per your current situation, with the understanding that we will be moving ahead with the projects on the timelines we have discussed I have been able to get approval to move forward with the discounted rate of $9000 per month for the FSMA on a month a month to month term beginning September 1. If you can confirm with email approval I will have it revised to the new rate.
>
> *Serinus to SysGen*: Can you confirm that we will still receive the same service as prior only we won't have a full-time onsite resource?
>
> *SysGen to Serinus*: Exactly, we would continue with the existing schedule of having a resource on-site in the morning and remote support in the afternoon.
>
> *Serinus to SysGen*: I approve us moving forward at the new rate. Also, will we receive a discount for July and August on our full fee given we didn't have an FTE on site?
>
> *SysGen to Serinus*: We were operating under the understanding that this would be updated when a new agreement was signed off. Although we adjusted the on-site support internally we were still dedicating just as many resources to your organization. In light of you not being able to sign a long term agreement I was able to fight for a special discounted approval moving forward but not to have it backdated.

[113] There is no evidence that the parties further discussed the FSMA Amendment. Its terms were finally accepted when Serinus paid the SysGen invoices with the $9,000 monthly fee.

[114] Serinus acknowledges that the plain, grammatical, and ordinary meaning of the FSMA Amendment indicates that the price of the FSMA was reduced on a month-to-month term, rather than the term of the FSMA being amended. However, it argues that the surrounding circumstances

negate only a month-to-month price reduction and also support a month-to-month term of the FSMA. I disagree.

[115] The surrounding circumstances are used to interpret the words used by the parties, not to overwhelm the words used or to see if they "negate" the plain words used, as argued by Serinus. I find that surrounding circumstances to the FSMA Amendment, and the unambiguous words used in the email exchange comprising the FSMA Amendment, interpreted as a whole and in context, support an interpretation that the parties only amended the price under the FSMA on a month-to-month basis, which was referred to by a non-lawyer in an email as a "month a month to month term".

[116] The parties had earlier explored a completely revised FSMA relationship. When that did not work, Serinus confirmed that the FSMA would remain in place and asked when it could expect the On-Site FTE. SysGen then offered a reduced price in return for not having to provide an On-Site FTE, but rather to continue the schedule of on-site morning support and remote support in the afternoons, even though SysGen had to dedicate the same resources to Serinus either way. The entire email exchange is about the "new rate" for the change in services. There is no objective evidence that the parties exchanged communications about changing the term or termination provisions of the FSMA.

[117] In fact, SysGen's proposal expressly confirmed the discounted rate "*for the FSMA*", which is a clear incorporation of the FSMA's terms but at a new price. SysGen stated that if Serinus confirmed with email approval, SysGen would have "it revised" to the new rate, which is a reference to revising the FSMA. After confirming Serinus will receive all the same services except the changes to the On-Site FTE, Serinus approved moving forward "at the new rate", but did not reference any other changes to the FSMA. When interpreted in the context of the entire email exchange and the surrounding circumstances, the reference to "on a month a month to month term beginning September 1" is a reference back to the price and not the term or termination provisions of the FSMA.

[118] This interpretation of the FSMA Amendment is also consistent with surrounding circumstance that Serinus did not want a long-term arrangement — under the confirmed terms of the FSMA it could decide to terminate the FSMA before its automatic renewal of the FSMA in January 2020. Serinus' obligations were short-term.

[119] Further, the revised price made commercial sense in the circumstances. The parties knew that Serinus was not looking for a long-term arrangement. Whether it would continue the FSMA in January 2020 was, therefore, up in the air. SysGen was offering an 18% discounted price even though the parties both knew that SysGen's information was that it dedicated the same resources without the On-Site FTE as it did with it. It made business sense that the parties agreed to a temporary price reduction until the parties knew whether the FSMA was continued for another year. I reject Serinus' argument that the change to the price could not have been intended to be on a monthly term because the reason for the price reduction was permanent.

[120] Accordingly, I find that the FSMA Amendment amended the price and on-site support services of the FSMA but otherwise confirmed its terms.

3. The FSMA's Disputed Clause and the Termination Letter

[121] The FSMA provided:

> Yearly Budgeted Maintenance
>
> All FSMA services are contracted for a period of 12 Months commencing on January 12, 2016 (the "Commencement Date"). This Agreement will be automatically renewed on each subsequent anniversary of the Commencement. Termination of this Agreement or of any renewal thereof must be received by SysGen on or before the subsequent renewal date. Early termination of the agreement must be presented as notice in writing, as such it is agreed SysGen Solutions Group will require 90-day notice for transition of services.
>
> (**Disputed Clause**)

[122] Serinus argues that the 90-day notice period referenced in the Disputed Clause only applies if Serinus (not SysGen) terminates the FSMA prior to its term coming to an end. It argues that SysGen does not get the benefit of the 90-day notice period if SysGen terminates the FSMA.

[123] In Serinus' correspondence on April 20 and 23, 2020, Serinus took the position that the FSMA did not provide SysGen any termination rights whatsoever, and that SysGen had ended the FSMA when it resigned on January 31, 2020. In oral argument, initially Serinus took the position the FSMA was terminated on January 31, 2020, but then acknowledged that there should be some notice of a transition period but the question was what a reasonable period would be. In its Reply Brief, Serinus took the position that, under the FSMA, SysGen was entitled to one-month (or thirty days) notice for transition of services, but then also took the position that Serinus' request that SysGen remove its LabTech RMM Software on April 2, 2020 marked the "official end" of the transition of services.

[124] Serinus' argument is that the reference to termination of the FSMA or any renewal thereof being "received by" SysGen in the second sentence, and the reference to SysGen requiring "90-day notice" for transition of services, only contemplates delivery of notice to SysGen and, therefore, the early termination provisions are a "one-way valve" that only apply when Serinus seeks early termination. I disagree with Serinus' interpretation.

[125] The Disputed Clause is titled "Yearly Budgeted Maintenance", which suggests part of the purpose of the clause is to give both parties some certainty on an annual basis as to what their costs and obligations will be.

[126] Interpreting the Disputed Clause as a whole, in that context, and in the context of the entire FSMA, the Disputed Clause deals with three distinct concepts. The first sentence addresses the initial term of the FSMA. The second and third sentences address the automatic renewal of the FSMA for subsequent one-year periods. Those sentences provide that the FSMA will be renewed automatically unless Serinus notifies SysGen of its choice that the FSMA will terminate on its end date — Serinus is not required to provide SysGen with advance notice of its choice, because it only has to notify SysGen "on or before" the renewal date. If Serinus fails to notify SysGen of its choice, then the FSMA is automatically renewed. The requirement that Serinus notify SysGen of

a decision to renew is informational only because the FSMA will renew automatically if Serinus does nothing. Notably, the notice requirement here is not formal, does not have to be in writing, and the default is renewal for another yearly term.

[127] As Serinus argues, I agree that the last sentence of the Disputed Clause deals with a different situation: early termination of the FSMA before the end date of the then current term. This sentence does not limit the early termination right to only one party.

[128] Parties to a business relationship would usually not intend to be bound in perpetuity: ***Rapatax (1987) Inc v Cantax Corporation Ltd***, 1997 ABCA 86 at paras 18–19; ***Conseil Scolaire Catholique Franco-Nord v Nipissing Quest (Municipalité)***, 2021 ONCA 544 at para 30. Whether the parties intended a contract to be of perpetual duration is a matter of interpretation of the agreement and its surrounding circumstances: ***Conseil Scolaire Catholique*** at para 33, citing ***Shaw Cablesystems (Manitoba) Ltd v Canadian Legion Memorial Housing Foundation (Manitoba)***, 1997 CanLII 11521 (MBCA), 143 DLR (4th) 193; ***Edmonton Kenworth Ltd v Kos***, 2018 ABQB 439 at para 43.

[129] In my view, based on the FSMA, the FSMA Amendment, and the surrounding circumstances, I find that the parties did not objectively intend their business relationship embodied in the FSMA to be a perpetual contract or one of indefinite length for SysGen but not for Serinus. That is, I interpret the FSMA as providing both parties the right to early termination. Under this provision, because it is a termination outside the annual planning by the parties, a more formal notice in writing is required.

[130] Accordingly, I interpret the 90-day notice requirement as applying to both parties. Contrary to Serinus' argument, unlike the earlier sentences in the Disputed Clause which deal with termination or renewal at the end of the term (which provided expressly for the notice being "received by SysGen"), the notice provision for early termination only talks about the "90-day notice" being "required" by SysGen (not received by SysGen). 90 days is the agreed notice period for early termination. It is not a "one-way valve" as argued by Serinus. It was the time SysGen required to transition services to a new IT service provider, regardless of which party terminated the FSMA.

[131] A problem with Serinus' interpretation is that it focusses on what it perceives to be the equities *now*, or at the time of the Termination Letter, and refers to SysGen as receiving the benefit of, or an entitlement to, a notice period. Serinus ignores the fact that the requirement to provide advance notice of early termination could just as easily have worked against SysGen's interest depending on the circumstances. Further, Serinus ignores that a notice period, in many situations, would provide a benefit to the customer, Serinus, to give it time to find a new IT provider without having a gap in critical IT support. In my view, the FSMA cannot objectively be interpreted to provide that SysGen could simply terminate the FSMA without notice and walk away. Accordingly, I interpret the reference to "90-day notice" as the notice period for both parties for early termination, because it was required for SysGen's transition of services to a new IT provider.

[132] Accordingly, I find that the Termination Letter was not an immediate resignation as argued by Serinus, but was a notice of early termination in writing providing 90-days' notice as contemplated by the FSMA. Therefore, the FSMA remained in place during the notice period,

subject to its possible earlier repudiation and termination by SysGen as discussed elsewhere in these Reasons.

[133] If I am wrong in my interpretation, and the 90-day notice period only applies to the notice period if Serinus exercises its right to early termination, then the agreement is silent on the notice period SysGen is required to provide to Serinus (if any). In this instance, Serinus acknowledges some notice period should apply, and argues for a 30-day period.

[134] If a court is satisfied that a reasonable notice period applies or should be implied, what is reasonable will depend on the circumstances of each case, including such factors as the expectations of the parties, the duration or intended duration of the relationship, the dependency of the terminated party on the arrangement and the commercial climate: ***1193430 Ontario Inc v Boa-Franc Inc***, 2005 CanLII 39862 (ONCA), 78 OR (3d) 81 at para 45; ***1397868 Ontario Ltd. v Nordic Gaming Corporation (Fort Erie Race Track),*** 2010 ONCA 101 at para 13.

[135] In this case, the parties' expectations were that the overall relationship was to be evaluated on an annual basis, and that it may require 90 days to effect a transition of IT services to a new provider, during which period Serinus would have some continued need for SysGen services. In the circumstances, if I was implying a reasonable notice period for SysGen to terminate the FSMA, I find the 90-day period is reasonable and the overall result would be the same.

4. Did SysGen Breach the FSMA?

[136] The FSMA obligates SysGen to maintain the security of Serinus' IT environments without introducing new security risks. The issue is whether the Administrator Lockdown breached this obligation.

[137] "Security" has been defined as "the quality or state of being secure: such as (a) freedom from danger: SAFETY; (b) freedom from fear or anxiety ...: : https://www.merriam-webster.com/dictionary/security. "Cybersecurity" has been defined as "measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack": https://www.merriam-webster.com/dictionary/cybersecurity.

[138] In my view, SysGen's obligation to maintain security and to protect from danger or threats includes protecting Serinus from danger or threats imposed by SysGen. This obligation was of increased importance when one of the parties had given an early termination notice and the parties were working toward transitioning Serinus to a new IT service provider.

[139] SysGen argues that the Administrator Lockdown was implemented in response to a security threat to Serinus' IT system and, therefore, was performance (not breach) of the FSMA. In many ways, this is the crux of this action. On balance, I find that SysGen's evidence provides little support for its position, for several reasons.

a. SysGen's Evidence of When it First Learned of the Security Threat and Decided to Implement the Administrator Lockdown is Vague, Inconsistent and Unreliable

[140] Richardet's evidence is that Jordan told him "on or about April 20" that Administrator Access had been granted to "unknown third parties", changes had been made to Serinus' network, and new software had been installed, all without SysGen's knowledge or consent. Richardet stated that, upon learning that, he determined it was necessary to temporarily return to the Standard Set-Up to properly investigate the matter and ensure Administrator Access was not granted to unqualified persons. He admitted in questioning that this conversation could have been a day earlier or a day later.

[141] Jordan's evidence was also vague on timing. He deposed that "on or about April 20" he advised Richardet about surreptitious third-party access and changes to the Serinus IT system. In questioning, he also acknowledged that it could have been a day earlier or later. However, Jordan's evidence is that he advised Richardet about this issue *after* he learned that Mansouri was having difficulty with his Administrator Access. The objective evidence is clear that Mansouri's difficulty in obtaining Administrator Access occurred on April 21, not April 20.

[142] Jordan's evidence does not make sense: Mansouri's loss of Administrator Access was *caused by* the Administrator Lockdown instructed by Richardet, so it could not have been the impetus for Jordan's discussion with Richardet that led to Administrator Lockdown. Jordan's discussion with Richardet must have occurred *before* the Administrator Lockdown. Jordan's evidence is unreliable.

[143] The timing of when Richardet instructed Swallow to implement the Administrator Lockdown, and the reason for the instructions, was also vague and unreliable. Both Richardet and Swallow said it was "on or about" April 20. Swallow's evidence, objectively supported by password logs, was that he performed the Administrator Lockdown on April 21, 2020 at 10:06 am. Further, it does not appear that Richardet informed Swallow of the reasons for the Administrator Lockdown: Swallow testified that he was not advised that there were changes being made to the Serinus IT system; he believed it was "just a request to make sure the systems were set up according to our best practice." Later, Swallow testified that he could not speak to what Richardet advised.

[144] None of Richardet, Jordan or Swallow kept any notes of their conversations that led or relate to the Administrator Lockdown. SysGen did not include any internal documentation in its evidence detailing the security threat or the planned response. Although SysGen had well-documented escalation processes and major security incident reporting procedures, there is no documented or objective evidence that any steps were taken by SysGen to document the implementation of those procedures with respect to the Administrator Lockdown.

b. The Stated Reason for the Administrator Lockdown is Not Compelling or Corroborated by Objective or Documented Evidence

[145] Again, SysGen's stated reason for the Administrator Lockdown was because Richardet learned that Administrator Access had been granted to "unknown third parties", changes had been

made to Serinus' network, and new software had been installed, all without SysGen's knowledge or consent. No specifics were provided about these matters in the evidence, and there is no documentation about them. It is important to put this into context.

[146] SysGen, and Richardet specifically, was well aware that Mansouri had been given Administrator Access by the end of January, 2020, almost three months before the Administrator Lockdown. Therefore, Mansouri could not be the unknown third party having Administrator Access that caused concern.

[147] SysGen also referenced in argument that Serinus provided access to persons in Romania, however this occurred in February 2020, and I find that SysGen knew about that around that time given that it continued to provide FSMA Services and had Administrator Access to Serinus' systems.

[148] Further, SysGen was aware that the transition of services would require cooperation and coordination with a new IT service provider, and that the new IT service provider would need Administrator Access. Serinus had retained IT Ops to assist it with its IT needs, and SysGen had in fact been aware since early March that Serinus had retained a new IT service provider. Jordan was specifically aware that Serinus' new IT provider had Administrator Access and that changes were being made to Serinus' IT system since March 4, 2020, because it was reported to him that:

> Sanad just called to advise me that their new IT is onsite and has access to quite a bit of the infrastructure as [Mansouri] has been backdoor resetting passwords. Sanad overheard their new IT discussing how they have implemented group policies and "pushed out their agent". It also sounds like they've set up a ticketing system.

[149] By at least March 15, 2020, SysGen knew both the identity of the new IT service provider as IT Ops and that Idris was IT Ops' representative.

[150] SysGen was aware of these various steps by March 2020, but did not lock the Serinus system down or take any other steps until much later. Kayser's opinion was that an IT service provider that is aware of a threat should act reasonably promptly. He also agreed that if there appears to be intrusions with unknown third parties accessing a system, the person responsible for the system should take action right away, not months later. SysGen took no steps to lock down the system after learning about Mansouri's access or the involvement or access of IT Ops and never raised any concerns with Serinus about it.

[151] Further, Jordan testified that SysGen did not perceive Mansouri and Serinus' new IT provider having access as a security threat. Rustom testified that he *did* consider it a security threat and that is why he reported it to other SysGen personnel; Rustom confirmed, however, that it did not usually take SysGen 40 days to respond to a security threat. Rustom confirmed he was not aware of any new security threats arising after early March 2020.

[152] In my view, it is not plausible and I do not accept SysGen's evidence on the balance of probabilities, that Mansouri and IT Ops (specifically Idris) having Administrator Access, or any other matter known to SysGen by mid March 2020, suddenly created an urgent or new security threat on April 20 or 21, 2020 that SysGen was not already aware of. SysGen had acquiesced in

the state of affairs for several weeks. I note that, according to the objective logs, the specific named account users that were subject of the Administrator Lockdown included Mansouri and Idris' accounts.

[153] Further, SysGen was aware that Serinus had requested that SysGen remove SysGen's RMM Software from Serinus' system in early April. Kayser confirmed that this is indicative of Serinus transitioning its services to a different provider and not wanting SysGen to have remote monitoring or access to Serinus' environment. Notwithstanding that, SysGen does not appear to have fully completed that task by April 2020. SysGen would likely have been aware that Serinus or its new IT service provider would need to install different software to have someone other than SysGen to remotely access Serinus' system. It seems unlikely that new software on the system suddenly gave rise to a concern about a new security threat, or that SysGen would proceed with an Administrator Lockdown without at least asking some questions about that new software.

[154] Finally, SysGen's evidence was vague — Jordan did not identify when he first learned of the concerning new software. As noted, Rustom was not aware of any new threats since early March 2020. SysGen, who was still obligated to be continuously monitoring Serinus' system, would likely have had a precise record of when any new concerning software was installed. On balance, there is insufficient evidence, and I do not accept, that new software had been installed on Serinus' IT system shortly before the Administrator Lockdown that created an urgent or new security threat that required immediate response.

c. SysGen Did not Reach out to Serinus Before or Immediately After Conducting the Administrator Lockdown

[155] SysGen conducted the Administrator Lockdown without notice to Serinus. If SysGen was concerned about unknown third-party access or new software, one would expect an immediate communication to Serinus to ask it what was going on or if Serinus knew anything about it (much as Serinus did when the Administrator Lockdown occurred and Serinus did not know what was going on). Even if it was a security emergency, one would have expected a notification from SysGen to Serinus about what had occurred, or at least some communication explaining or updating matters as information became known. Both experts generally agreed on this point. But that is not what SysGen did. Instead, Serinus was left to discover the Administrator Lockdown on its own.

d. April 21, 2020: SysGen's Response to Serinus' Questions About the Administrator Lockdown is Vague and Delayed

[156] The communications by and between Serinus and SysGen after Serinus became aware of the Administrator Lockdown are telling. The objective records show Serinus and IT Ops expeditiously trying to figure out what is going on, and SysGen vaguely and slowly responding.

[157] On April 21, 2020 at 2:01 pm, about two hours after Mansouri first discovered something was amiss, Mansouri reached out to Pentlichuk and asked SysGen if it had any group policy objective or software that was responsible for the loss of Administrator Access. Mansouri emailed him again 10 minutes later, and again at 2:43 pm, asking who Swallow was and whether Swallow was investigating the issue. At 2:48 pm, Pentlichuk stated:

> I am working with Shane and Sanad regarding this. Yes, Mike Swallow is a SysGen employee. I have also reached out to Mike to discuss your question and situation. We will have a response to you soon.

[158] Almost three hours later, Mansouri follows up with Pentlichuk for an update of the diagnosis of the situation. It then took Pentlichuk another hour and a half to respond and said: "Shane updated me and let me know that they are investigating and working it. I will keep you posted as they let me know".

[159] Mansouri did not hear back from SysGen that day.

[160] SysGen's approach here is concerning. The reference in Pentlichuk's email to "Shane" is a reference to Jordan, who was well aware of why the Administrator Lockdown had occurred. If Jordan had advised Pentlichuk about that, it is of concern that Pentlichuk did not simply tell Mansouri what SysGen knew about what was going on. If Jordan had not advised Pentlichuk about the reason for the Administrator Lockdown, this is also concerning and suggests that Jordan did not want Pentlichuk to know the reason for the Administrator Lockdown. In either instance, and in any event, I find this evidence inconsistent with SysGen responding to a real security threat.

e. April 22, 2020: SysGen Deletes Serinus' Software

[161] Early on April 22, 2020, Mansouri notified Pentlichuk that he had been able to identify that the Administrator Lockdown had been through the "Waterboy" account. He wanted to know why Swallow appeared to have access when administrator credentials had changed. Mansouri ended his email by highlighting the seriousness of the situation: "Please let me know because this is a very high level security issue for our infrastructure". SysGen's lack of response to this email is concerning and is not consistent with responding to a security threat.

[162] Also concerning is that, after Mansouri's email to Pentlichuk, and at a time that only SysGen had Administrator Access, SysGen deleted Serinus' Altera and other software necessary for Serinus to manage its IT system. SysGen did not notify Serinus or ask for its permission to remove this software before it deleted it. Mansouri was frequently in email communication with SysGen that day and was actually awaiting a response from SysGen to his questions. If this deleted software had been part of SysGen's security concerns, one would have expected at least an email about it before it was deleted. Further, based on Swallow's evidence, deletion of the software was not part of what Swallow was originally instructed to do — he had been instructed to return to the Standard Set-Up. The deletion of Serinus' software on April 22, 2020 was not reasonably explained by SysGen in its evidence.

f. April 22 and 23, 2020: SysGen Misleads, Obstructs and Further Delays Responses

[163] On April 22, 2020, Mansouri made a service request to Swallow: "we are unable to use admin accounts, can you reset" the Mansouri and Idris accounts. Swallow reset the passwords, but failed to explain to Mansouri that he was only resetting their end-user access which would give them access to their emails, not Administrator Access even though that is what Mansouri expressly requested. Mansouri then stated to Swallow: "...I think my account doesn't belong to admin

domains accounts anymore"? Swallow's response was "I can confirm the system is clean but we're monitoring security closely right now to ensure there are no problems".

[164] Swallow's response is concerning. Although he knew that he personally removed Administrator Access to both Mansouri and Idris's accounts, he did not disclose that in response to Mansouri's emails. Further, he did not clearly bring it to Mansouri's attention that he was not actually resetting Administrator Access but only end-user access. When questioned about this, he vaguely states that the system is clean, but does not explain why he is not reinstating the Administrator Access.

[165] I find that Swallow's emails were misleading, failed to do what Mansouri asked of him, failed to explain that he had not done what was asked of him (restoring Administrator Access), and failed to explain *why* he had not done what was asked of him. If the purpose of the Administrator Lockdown and the reason SysGen continued to "monitor security closely" was due to a security threat, SysGen would likely have provided some details to its obviously distressed client.

[166] Serinus (Mansouri) spoke to SysGen (Pentlichuk) on April 23, 2020, advising that Serinus needed Administrator Access services back and running, and requesting that the Administrator Access be kept out of any management dispute. SysGen provided no response after that conversation.

[167] Further, on April 23, 2020, Serinus formally demanded SysGen to immediately confirm whether the Administrator Lockdown was undertaken by SysGen or with its knowledge. SysGen did not respond. It knew exactly what happened and why, and I find would likely have explained it immediately if it was due to a perceived third party security threat.

g. The Timing of the Dispute Letter, the Administrator Lockdown and the Offer, is Unlikely a Coincidence

[168] Serinus emailed the Dispute Letter to SysGen at 7:35 am on April 21, 2020. Less than three hours later, SysGen implemented the Administrator Lockdown. In his questioning, Jordan denied that the Dispute Letter had anything to do with the decision to implement the Administrator Lockdown.

[169] However, Richardet could not remember whether he received the Dispute Letter before or after he instructed the Administrator Lockdown. Richardet also confirmed in questioning that he was aware there was a dispute respecting billing prior to seeing the Dispute Letter. I find he was aware of the existence of the Billing Dispute before instructing the Administrator Lockdown.

[170] Richardet also gave this evidence in questioning:

> Q. Well, and I understand that that's your position, sir. Right, and so your first reaction - if you're telling me this - on your having this conversation with Mr. Jordan, was to instruct Mr. Swallow to reset all administrative passwords, not to contact Serinus; correct?

A. I did not instruct him not to contact Serinus. I believed he was in contact with Serinus. I've seen some e-mails that would suggest he was in contact with Serinus. I had no reason to believe he wasn't in contact with Serinus. So he was -- he was, you know, instructed to, you know, return to our standardized position with locking the environment down and to investigate what was going on there. And, you know, I had subsequent conversations with Mr. Swallow to try and identify what the software was, but we could not identify what that was.

And as far as -- you know, billing issues come and go. Like I did not believe at the time that there was some insurmountable billing issue that we couldn't get our heads around. Even to the point of, you know, when Mr. Auld terminated us, I mean I didn't -- I did not anticipate that because of a billing issue.

I'm very good at resolving billing issues. As a matter of fact, I can tell you that, you know, our standing performance in collecting money is exceptional. And, you know what, I'm very, very good at that. So I was not threatened by that at all.

Q. Sir, how many times have you refused to provide administrative access to your clients to their systems until they paid you?

A. Several.

[171] By April 24, 2020, SysGen had not provided any substantive information to explain the Administrator Lockdown. Serinus demanded through counsel that its access be restored immediately. SysGen's response to that demand is not consistent with a response to a security threat. Instead of restoring Serinus' Administrator Access or explaining the security threat and why it could not restore its access, SysGen sent a settlement offer about the Billing Dispute. While the actual offer is not in evidence before me, in its written argument Serinus states that the offer was "to resolve the Billing Dispute" and SysGen stated that the offer was "to return administrative access to Serinus". Neither party objected to these references being before me. It is clear from these references, and by logical inference, that the offer involved and somehow tied together the return of the Administrator Access and resolution of the Billing Dispute. In my view, this is not behaviour consistent with responding to a security threat. It is a negotiation strategy.

[172] Richardet confirmed in his questioning that, over the weekend, SysGen had decided to simply end the relationship on Monday, April 27, 2020. I find that this would require returning Administrator Access to Serinus and, therefore, that SysGen must have believed at that time that there was no security threat. However, SysGen did not notify Serinus of its intentions to reinstate Administrator Access and did not actually reinstate access before Serinus completed the Serinus Restoration. Instead, as Richardet stated in questioning: "and we were waiting back for, you know, a response on the offer we had made".

[173] In the early morning of April 27, 2020, SysGen (Pentlichuk) notified Serinus (Mansouri, Yaniw and Auld) that "there is a service hold on Serinus' account with SysGen because of a billing dispute. Before you and I are able to resolve IT items, the account must be cleared up". While

Serinus had already regained Administrator Access by this point, it had not yet advised SysGen. Pentlichuk's email indicates that SysGen continued to link resolution of IT issues to the Billing Dispute on April 27, 2020.

[174] SysGen's behaviour, when viewed on the balance of the evidence, was inconsistent with responding to a security threat. It was consistent with settlement strategy.

5. Conclusion re: SysGen Breach of Contract

[175] Based on the evidence before me, and the above review, I do not accept and give little-to-no weight to SysGen's evidence that it implemented the Administrator Lockdown due to a perceived security threat.

[176] Instead, I find on the balance of probabilities:

(a) SysGen received the Serinus' Dispute Letter early on April 21, 2020;

(b) SysGen (Richardet and Jordan) immediately decided to implement the Administrator Lockdown, and Richardet instructed Swallow to do so;

(c) SysGen knew or ought to have known there was no actual or new security threat to Serinus' system, because it had been aware of Mansouri and IT Ops' Administrator Access for weeks, and it knew or ought to have known that the transition to a new IT service provider would involve making changes to Serinus' IT system and installing software to be used by new administrators;

(d) the Administrator Lockdown was not implemented to address an actual or new security threat that SysGen was concerned about or believed existed, but rather was in response to the Dispute Letter and as part of its collection and Billing Dispute strategy — a strategy it appears to have used with other clients previously;

(e) the Administrator Lockdown was not performed as part of the FSMA Services or otherwise authorized by Serinus; and

(f) in conducting the Administrator Lockdown, SysGen inserted a security threat into Serinus' IT system, namely SysGen itself, for the purposes of extracting benefit for SysGen to the detriment of Serinus in respect of the Billing Dispute.

[177] Accordingly, I find that SysGen breached its obligations under the FSMA and is liable to Serinus for breach of contract. Further, I find that the Administrator Lockdown constituted a repudiation of the FSMA. SysGen's conduct evinced "an intention not to be bound" by the FSMA: ***Guarantee Co of North America v Gordon Capital Corp***, 1999 CanLII 664 (SCC), [1999] 3 SCR 423 at para 40; ***Globex Foreign Exchange Corporation v Kelcher***, 2011 ABCA 240 at para 46. I address repudiation further later in these Reasons.

[178] Although not specifically pleaded, and not necessary to make out the breach of contract claim, had it been pleaded I would have found that SysGen breached its obligation under the 2010 Application agreement to make reasonable attempts to clarify issues with invoices. The Administrator Lockdown was not a reasonable attempt to clarify the Billing Dispute.

[179] Serinus did not specifically plead a breach of the duty of honest performance, or a breach of the duty to exercise contractual discretion in good faith, as contemplated respectively in ***Bhasin v Hrynew***, 2014 SCC 71 and ***Wastech Services Ltd v Greater Vancouver Sewerage and Drainage District***, 2021 SCC 7. Accordingly, I make no further comment or findings about those potential claims, except in the context of punitive damages.

D. Is SysGen Liable for Conversion?

[180] The tort of conversion involves the wrongful interference with the goods of another, such as taking, using or destroying the goods in a manner inconsistent with the owner's right of possession: ***Boma Manufacturing Ltd v Canadian Imperial Bank of Commerce***, 1996 CanLII 149 (SCC), [1996] 3 SCR 727 at para 31; ***373409 Alberta Ltd (Receiver of) v Bank of Montreal***, 2002 SCC 81 at para 8. Conversion can occur in so many different circumstances that framing a precise definition of universal application is almost impossible: ***Driving Force Inc v I Spy-Eagle Eyes Safety Inc***, 2022 ABCA 25 at para 30, citing ***Kuwait Airways Corporation v Iraqi Airways Co (Nos 4 and 5)***, [2002] UKHL 19 at para 39, [2002] 2 AC 883.

[181] The Court of Appeal has confirmed that one way of summarizing the test is found in ***Clow v Gershman Transport International Ltd***, 2000 ABQB 360 at para 13, namely: (a) a wrongful act; (b) involving a chattel; (c) consisting of handling, disposing or destruction of the chattel; (d) with the intention or effect of denying or negating the title of another person to such chattel: ***Driving Force*** at para 31. I address these elements below.

1. Wrongful Act

[182] Dealing with another's chattel in a manner authorized by the rightful owner will not constitute a wrongful act: ***Driving Force*** at para 33; ***373409 Alberta*** at para 9.

[183] Kayser's opinion that SysGen's Administrator Lockdown was authorized was based on his legal interpretation of the contractual arrangement (which he was not qualified to make), and a fundamental assumption that is not borne out in the evidence — that SysGen had been made aware that an additional third party had been given administrative rights that SysGen was not previously aware of. Kayser did not opine on whether the Administrative Lockdown was in accordance with industry standards. Mathezer also operated under the incorrect assumption that SysGen had resigned effective January 31, 2020. I do not give weight to either expert's opinion whether SysGen was authorized to conduct the Administrator Lockdown.

[184] Serinus owned its IT systems, but SysGen continued to have access to those systems during the transition period so it could continue to provide FSMA Services while it also transitioned the FSMA Services. However, Serinus had previously demanded that Mansouri be given Administrator Access in January, and Mansouri was given that access. Further, to SysGen's knowledge, Serinus had granted IT Ops Administrator Access as part of the transition of services. SysGen knew that Serinus and IT Ops having Administrator Access was required for the transition of services. Serinus had asked SysGen to remove its RMM Software. SysGen did not seek Serinus' consent or authorization to remove Serinus' and IT Ops' Administrator Access or to delete software. I have found it was in breach of the FSMA for it to implement the Administrator Lockdown.

[185] I find SysGen committed a wrongful act as required for a conversion claim.

2. Involving a Chattel

[186] While traditionally conversion involved tangible goods, courts have recognized that interference with an owner's electronic information, or the owner's access to electronic information, can also constitute conversion. For example, in ***Prim8 Group Inc v Tisi***, 2016 ONSC 5662, the court held that a person preventing access to another party's software could be conversion. In ***Canivate Growing Systems Ltd v Brazier***, 2020 BCSC 232, the court held that electronic data in the form of a website or an email address, or intellectual property, could be the subject of conversion. In ***Canivate*** the court stated:

> [71] In the electronic age in which we live, I find that it would be incongruous if conversion were limited to physical goods, or tangible chattels. In the case at bar, the defendant exerted exclusive control over Canivate's website as soon as he removed administrative control of *canivate.com* from the company. The defendant held the only key to the website which was critical to operations of the company, and prevented Canivate from using its website and email addresses. I find that a modern conception of conversion must include wrongful interference with intangible goods, such as electronic data, websites and email.
>
> [72] This modern understanding of the application of the law of conversion is consistent with the law stated by United States Court of Appeals, Ninth Circuit in *Kremen v. Cohen*, 337 F.3d 1024 (9th Cir. 2003) at 1030 [*Kremen*] in which the court recognized the conversion of intangible property, specifically domain names.
>
> [73] Caitlin Akins, in "Conversion of Digital Property: Protecting Consumers in the Age of Technology" 23 Loyola Consumer Law Rev. 215 (2010) at 235, discusses *Kremen*, and a subsequent decision of the New York Court of Appeals in *Thyroff v. Nationwide Mutual Insurance Co*, 864 N.E. 2d at 1273, summarizing the New York Court of Appeals' discussion as follows:
>
> > In its discussion, the court listed four reasons why the digital chattel at issue should be recognized for the purposes of conversion. First, there must be a civil remedy to accompany the criminal charge of theft in some cases. Second, virtual documents are only a button push away from being printed and manifested as tangible chattels. Third, in a philosophical sense, writing is writing, no matter what form it takes; and writing is a form of property. Fourth, there must be a way to recoup the expenses of creating digitized possessions. Elaborating on the practical realities of virtual documents, the court also concluded that it is not a document's or idea's physical manifestation that determines its worth, but the value of its content.
>
> [74] I find the reasoning articulated in the passage above to be directly applicable to the case before me.

[187] I agree with these cases and, if necessary, apply them. In this case, Serinus' owned IT systems, including its Calgary IT server, or parts thereof, are chattels that could be the subject of conversion.

3. Handling, Disposing or Destruction of a Chattel

[188] Preventing access to an owner's property can constitute handling or using of the property to give rise to conversion. In the context of electronic information, software, or databases, this can include preventing the owner's access to its property: ***Prim8*** at para 38; ***Canivate*** at paras 67–75.

[189] SysGen argues that, in order for conversion to exist, there must be some use made of the goods or some dealing with them, and that a short-term "seizure" of goods is insufficient, relying on ***384238 Ontario Ltd v Canada***, 1983 CanLII 5076 (FCA), 8 DLR (4th) 676 and ***Clow***. In ***Clow***, Justice Paperny (as she then was) held that a bailiff seizing a vehicle and transporting it to a third party storage facility did not demonstrate any intention to exercise dominion over the vehicle. In ***384238 Ontario***, the defendant wrongfully seized the plaintiff's goods and retained them for three days and this did not constitute conversion.

[190] This case is distinguishable from ***Clow*** and ***384238 Ontario***. I find that this was not a simple, short-term seizure of goods by a third party to safeguard them. SysGen's Administrator Lockdown reset passwords within the Serinus IT systems and changed its settings to remove Serinus' Administrator Access. I have found it was not for the purpose of safeguarding Serinus' system, but rather as part of a settlement strategy. The reason that Serinus was locked out for only a few days was because Serinus managed to break back into its own system. While Richardet testified that he was planning to return access on April 27, 2020, the only objective evidence is that on April 27, 2020 SysGen's position was that IT issues could not be resolved until the Billing Dispute was resolved.

[191] In all the circumstances, I find SysGen handled and used Serinus' property sufficiently to support Serinus' conversion claim.

4. With the Intention or Effect of Denying or Negating the Title of Another Person to Such Chattel

[192] After the Administrator Lockdown, Serinus users continued to have end-user access to the Serinus systems. However, Serinus could no longer effect any changes to the system that required administrator-level authorization. By removing Serinus' ability to make changes, SysGen effectively prevented Serinus from exercising its rights to possess and control (including by changing or updating) its own IT systems, which I find had the effect of denying Serinus the full incidents of title and ownership of its systems. SysGen then used the incidents of ownership and possession associated with the Administrator Lockdown for its own benefit — as a bargaining chip in the resolution of the Billing Dispute.

[193] This case is analogous to ***Prim8*** and ***Canivate***, where the plaintiffs owned and controlled, but then were locked out of, their software, website contents and emails. It is distinguishable from ***Del Guidice v Thomson***, 2021 ONSC 5379, where the court held that individuals did not have control over their names contained on a financial services corporation's server.

5. Conclusion re Conversion

[194] Based on the foregoing, and considering all the evidence, I find that SysGen wrongfully interfered with Serinus' property and used it in a manner inconsistent with Serinus' right of possession and ownership. I find that by implementing the Administrator Lockdown, SysGen committed the tort of conversion and is liable to Serinus.

E. Is SysGen Liable for Breach of Fiduciary Duty?

[195] Fiduciary duty is an equitable doctrine originating in trust — generally speaking a fiduciary is required to act in the best interests of the person on whose behalf it is acting, to avoid all conflicts of interest, and to strictly account for all property held or administered on behalf of that person: ***Manitoba Métis Federation Inc v Canada (Attorney General)***, 2013 SCC 14 at para 47, citing ***Lac Minerals Ltd v International Corona Resources***, 1989 CanLII 34 (SCC), [1989] 2 SCR 574 at 646–47.

[196] Fiduciary relationships may be either *per se* or *ad hoc*. The former refers to those relationships that the law presumes to be — and characterizes as — fiduciary: ***Professional Institute of the Public Service of Canada v Canada (Attorney General)***, 2012 SCC 71 at para 113; ***Galambos v Perez***, 2009 SCC 48 at paras 36–37. The recognized categories give rise to fiduciary duties because of their inherent purpose or their presumed factual or legal incidents: ***Professional Institute*** at para 113. The historically recognized *per se* fiduciary relationships are the traditional categories of trustee-*cestui que trust*, executor-beneficiary, solicitor-client, agent-principal, director-corporation, and guardian-ward or parent-child: ***Professional Institute*** at para 115; ***Alberta v Elder Advocates of Alberta Society***, 2011 SCC 24 at para 33.

[197] The existence of an *ad hoc* fiduciary relationship is determined on a case-by-case basis arising from the specific circumstances of a particular relationship: ***Professional Institute*** at para 113; ***Galambos*** at para 48; ***Elder Advocates*** at para 33.

[198] For an *ad hoc* fiduciary duty to arise, the claimant must show, in addition to the vulnerability arising from the relationship as described by Wilson J in ***Frame v Smith***, 1987 CanLII 74 (SCC), [1987] 2 SCR 99: (1) an undertaking by the alleged fiduciary to act in the best interests of the alleged beneficiary or beneficiaries; (2) a defined person or class of persons vulnerable to the fiduciary's control; (3) a legal or substantial practical interest of the beneficiaries that stands to be adversely affected by the alleged fiduciary's exercise of discretion or control: ***Elder Advocates*** at para 36; ***Williams Lake Indian Band v Canada (Aboriginal Affairs and Northern Development)***, 2018 SCC 4 at para 162 (Brown J in dissent); ***Manitoba Metis Federation*** at para 50; ***Breen v Foremost Industries Ltd***, 2023 ABKB 552 at para 385.

[199] In ***Abt Estate v Cold Lake Industrial Park GP Ltd***, 2019 ABCA 16 at para 73 and ***HRC Tool & Die Mfg Ltd v Naderi***, 2016 ABCA 334 at para 6, the Alberta Court of Appeal has described the *ad hoc* fiduciary relationship test this way:

(a) the fiduciary has scope for the exercise of some discretion or power;

(b) the fiduciary can unilaterally exercise that power or discretion so as to affect the beneficiary's legal or practical interests;

(c) the beneficiary is peculiarly vulnerable to, or at the mercy of, the fiduciary holding the discretion or power; and

(d) the existence of an undertaking by the alleged fiduciary to act in the best interests of the alleged beneficiary or beneficiaries.

[200] Mere vulnerability or reliance is not sufficient to create a fiduciary relationship: ***Elder Advocates*** at para 28; ***Abt Estate*** at para 73.

[201] A fiduciary relationship can exist in a commercial context: ***Indutech Canada Limited v Gibbs Pipe Distributors Ltd***, 2013 ABCA 111 at para 28. Having said that, fiduciary duties are rarer in the commercial context: ***Frame v Smith*** at 137–38; ***Lac Minerals*** at 595; ***Roorda v MacIntyre***, 2010 ABCA 156 at para 16; ***Hudson King v Lightstream Resources Ltd***, 2020 ABQB 149 at para 140; ***Ruel v Rebonne***, 2022 ABQB 271 at para 81. The terms of a contract can create the fiduciary relationship: ***Indutech*** at paras 29–35. However, the plaintiff must be able to point to a legal or practical interest that was not solely created by the contract (or existed regardless or independently of the contract), such as a property interest: ***Hudson*** at paras 137–39; ***Elder Advocates*** at para 35. Further, not every contractual obligation will give rise to a fiduciary duty: ***Hudson*** at para 139; ***Luscar Ltd v Pembina Resources Ltd***, 1994 ABCA 356 at para 68, 162 AR 35.

[202] Serinus has established three of four elements of the *ad hoc* test outlined by the Court of Appeal in ***Abt Estate***. Under the FSMA, SysGen was given access to Serinus' property (its IT systems). The FSMA did not mandate precisely how SysGen was to perform all of its obligations, including its obligation to maintain the security of Serinus' systems. Therefore, SysGen had some discretionary powers that could be unilaterally exercised to affect Serinus' legal and practical interests.

[203] Serinus also established the required express or implied undertaking. The party asserting the fiduciary duty must be able to appoint to a forsaking by the alleged fiduciary of the interests of all others in favour of those of the beneficiary, in relation to the specific legal interest at stake: ***Elder Advocates*** at para 31; ***Hudson*** at para 127. The FSMA provides that SysGen keep Serinus' IT internal structure and marketing strategies confidential, but does not speak to an undertaking to only act in Serinus' best interests in respect of Administrator Access and control of the IT system. However, in the Termination Letter, SysGen expressly undertook to work with Serinus "to transition services in an expeditious and professional manner". The transition of services included facilitating a changeover of responsibility for the protection of the Serinus IT system at a time when both parties were aware that the relationship was ending. By promising to act expeditiously and in a "professional" manner in those circumstances, I find that SysGen was undertaking to act in Serinus' best interests to the exclusion of all other interests as administrator control over Serinus' property was being transitioned back to Serinus.

[204] However, I find that Serinus was not peculiarly vulnerable to SysGen and has not made out an *ad hoc* fiduciary relationship. Serinus was a sophisticated commercial entity and had exhibited that it was both willing and able to strongly assert its rights and positions against SysGen. Further, SysGen had demonstrated that it would defer to Serinus' demands. In fact, it was Serinus demanding to have Administrator Access that caused SysGen to terminate the relationship. Further, since January 2020, and during the notice period following the Termination Letter,

Serinus actually had Administrator Access. Serinus could have protected itself by further restricting SysGen's access and powers before the Administrator Lockdown. Finally, Serinus showed that it had the ability to regain access to its systems through the Serinus Restoration.

[205] In all the circumstances, I find that Serinus has not established an *ad hoc* fiduciary relationship and its fiduciary duty claim is dismissed.

F. Is SysGen Liable for Intrusion Upon Seclusion?

[206] Serinus acknowledges that Alberta courts have been reticent to recognize the tort of intrusion upon seclusion, citing ***Papaschase First Nation v McLeod***, 2021 ABQB 415 at para 41; ***Kang v MB***, 2019 ABQB 246 at para 153. Further, this Court, and the Alberta Court of Appeal, have affirmed that there is no common law cause of action for breach of privacy in Alberta: ***D(SJ) v P(RD)***, 2023 ABKB 84 at para 15; ***Benison v McKinnon***, 2021 ABQB 843 at para 12; ***Al-Ghamdi v Alberta***, 2017 ABQB 684, aff'd 2020 ABCA 81.

[207] Serinus argues that it is time for this Court to recognize the tort of intrusion upon seclusion pursuant to the principles set out by the Supreme Court of Canada in ***Nevsun Resources Ltd v Araya***, 2020 SCC 5 at paras 118–23. A key question in recognizing a new tort is whether the harm in question cannot be adequately addressed by recognized torts: ***Nevsun*** at paras 123, 237; ***Alberta Health Services v Johnston***, 2023 ABKB 209 at paras 83–85.

[208] In this case, I have already found that SysGen's conduct constituted breach of contract and the tort of conversion. Even if it might be possible, this is not the appropriate case to consider recognizing a new tort and I decline to engage in the ***Nevsun*** analysis.

G. If SysGen is Liable to Serinus, What are Serinus' Damages?

[209] Serinus claims both compensatory damages and punitive damages.

1. What are Serinus' Compensatory Damages?

[210] Serinus claims as compensatory damages: (1) internal personnel costs; (2) amounts paid to iON for the iON Work; (3) general damages; and (4) aggravated damages.

[211] The principles of ***Hadley v Baxendale*** (1854), 9 Exch 341, 156 ER 145 continue to govern damages for breach of contract. In ***Dow Chemical Canada ULC v NOVA Chemicals Corporation***, 2020 ABCA 320 at para 57 [***Dow Chemical Canada***], the Court of Appeal described it as follows:

> ... ***Hadley v Baxendale*** (1854), 9 Exch 341, 156 ER 145 held that on a breach of contract the damages that the plaintiff can recover are:
>
> > . . . such as may fairly and reasonably be considered as either arising naturally, i.e., according to the usual course of things, from such breach of contract itself, or such as may reasonably be supposed to have been in the contemplation of both parties at the time they made the contract as the probable result of the breach of it. If special circumstances under which the contract was actually made were communicated by the plaintiffs to the defendants, and thus known

> to both parties, the damages resulting from that breach of such a contract which they would reasonably contemplate would be the amount of injury which would ordinarily follow from a breach of contract under the special circumstances so known and communicated. . . .
>
> This set the test for foreseeability of damages for breach of contract. The recoverable damages are those that would be in the reasonable contemplation of the parties at the time of contract. There is only one rule, but if "special circumstances" have been communicated, then the damages within the parties' reasonable contemplation would be wider.

[212] I find that it would clearly be in the contemplation of the parties at the time of the FSMA, that if SysGen breached the FSMA by introducing a security threat into Serinus' IT systems, Serinus would immediately take steps to investigate the threat, regain access to its systems, and conduct a review to ensure that there were no remaining threats in the system.

[213] The traditional measure of damages for conversion is the market value of the chattels at the time and place of their loss, together with special damages which are not too remote: ***Klewchuk v Switzer***, 2003 ABCA 187 at paras 57–60.

[214] On these bases, I address Serinus' specific compensatory damages claims.

a. Serinus' Internal Personnel Costs

[215] Serinus claims $8,311.35 for the value of 78 hours of time its salaried employees spent responding to the Administrator Lockdown, based on an estimate of hours of various employees multiplied by an estimated dollar value of their time. Serinus did not incur additional employee costs because it did not pay the employees anything more than their normal salary. Some of the employee time was during regular working hours and took them away from their normal duties, and some of the time was not during regular working hours and those employees were not compensated for that extra time.

[216] In similar situations, the value of personnel costs incurred to regain access to electronic systems have been recoverable damages: ***Prim8*** at para 68; ***Canivate*** at paras 82–86.

[217] SysGen does not appear to challenge Serinus' estimates of time, but rather argues that Serinus' damages relate to Serinus taking an unreasonably risky step in performing the Serinus Restoration, or are too remote and unreasonable. SysGen argues, in any event, that Mansouri was able to take all necessary steps to respond to the Administrator Lockdown in 12 hours, or about $455.64.

[218] SysGen, including through Kayser, adduced evidence that a BFA is a risky step, and that the Serinus Restoration was a BFA. Serinus and Mathezer's evidence is that the Serinus Restoration did not employ a BFA, but Serinus does acknowledge the Serinus Restoration was risky and described it as a "break the glass procedure". I do not need to resolve the question of how to label the Serinus Restoration. The risks identified with a BFA did not come to fruition and

Serinus did not unreasonably compound its losses regardless of the characterization of the Serinus Restoration. In any event, both sides agree that the Serinus Restoration was risky.

[219] SysGen also suggests that Serinus misled SysGen by suggesting it was only going to pursue legal remedies, not try to break into its own system. I reject this argument because SysGen's April 24 letter was clear that Serinus planned to take whatever steps necessary to regain control of its systems, *including* (but not exclusively) seeking court assistance.

[220] Kayser agreed that losing Administrator Access would be a high level of concern, and that having administrator control in the hands of an unknown third party would require a higher level of attention. However, he refused to answer questions about whether Serinus taking urgent or immediate action was justified if it was assumed that SysGen implemented the Administrator Lockdown to get paid a disputed invoice. He was argumentative, difficult and became an advocate. He refused to answer questions that would have been helpful to the court. I give little weight to his opinion about whether Serinus acted reasonably in response to the Administrator Lockdown, including in performing the Serinus Restoration.

[221] In my view, it is not for SysGen, in hindsight, to be unduly critical of Serinus' response to the situation. A plaintiff who has suffered damage has an obligation to mitigate the damage by taking reasonable steps to avoid damage that could result from the defendant's conduct, but is only obligated to make an objectively reasonable decision which is not to be "nicely weighed in hindsight": ***Christianson v North Hill News Inc***, 1993 ABCA 232 at para 11; ***Calgary (City) v Costello***, 1997 ABCA 281 at para 42; ***623455 Alberta Ltd v The Partnership of Jackie Handerek & Forester and Shawn D Hagen***, 2018 ABQB 86 at paras 285–86; ***1406444 Alberta Ltd v Taylor***, 2020 ABQB 356 at paras 62–63.

[222] I find on the balance of probabilities that Serinus' response to the situation was reasonable in all the circumstances.

[223] Serinus is entitled to recover some of its internal personnel costs as damages, but the amount must be adjusted to reflect the fact that some of the time spent was in off-hours, because the time estimates appear high and likely intermingled with time spent on the Billing Dispute, and to reflect the fact that some of the employees were not paid in Canadian dollars.

[224] I find a reasonable amount of internal personnel costs is $5,000.

b. Amounts Serinus Paid to iON

[225] SysGen argues that Serinus should only be able to recover the costs it incurred to the point it had recovered its Administrator Access. I disagree.

[226] I find Serinus is entitled to all costs reasonably incurred responding to the situation, including work done after it had recovered Administrator Access to ensure that there were no remaining threats embedded in its system. At that time, Serinus was faced with a situation where it suspected (correctly) that SysGen had taken away its Administrator Access without notice or cause, and was not reasonably communicating with Serinus about the situation. It was reasonable for Serinus to do a complete assessment to ensure that SysGen or someone else had not taken

further steps to disrupt Serinus' business. I find that, in the circumstances, the steps Serinus took in response were reasonable and based on advice from both internal and external IT professionals.

[227] As noted earlier, I have not admitted or relied upon any opinion of Mathezer as to whether the iON Work or associated costs were reasonable. However, I have reviewed iON's invoice and Mathezer's questioning about what exactly iON was doing.

[228] In addition to providing services that were in direct response to SysGen's conduct, while iON was in Serinus' system iON provided recommendations for improvements to Serinus' IT systems to reduce future security risks. The latter costs, valued at $11,911, are not directly attributable or arising out of SysGen's conduct, however, iON did not charge for those services, they were deducted from iON's account, and they do not form part of Serinus' claim.

[229] Accordingly, I find that the amount paid to iON was reasonably incurred and Serinus is entitled to $42,012.50, as outlined below:

Item	Description	Amount ($)
1	Cyber Incident Response - Darkweb Search	4,515.00
2	Discount	- 840.00
3	Cyber Incident Response - External Vulnerability Assessment	430.00
4	Discount	- 80.00
5	Cyber Incident Response - External Threat Intelligence Search	1,505.00
6	Discount	- 280.00
7	Cyber Incident Response - Digital Forensics on 3 Machines	25,800.00
8	Discount	- 4,800.00
9	Cyber Incident Response	17,200.00
10	Discount	- 3,200.00
11	Cyber Incident Response - Security Assessment and Recommendation	11,911.00
12	Discount	- 11,911.00
	Less Retainer already paid	- 5,000.00
	Subtotal	35,250.00
	GST	1,762.50
	Invoice Total	37,012.50
	Plus $5,000 retainer paid	5,000.00
	Grand Total	42,012.50

c. General Damages

[230] Serinus also seeks an amount for general damages. It points to the decisions of ***Canivate*** and ***Prim8*** as supporting its claim. ***Canivate*** involved the interference of a website which affected the plaintiff's branding and public relations. The court awarded $40,000 in general damages. ***Prim8*** involved a shareholder, officer and director removing computer and other equipment that contained development versions of client websites, without which the plaintiff's ability to service its client was disrupted. The court awarded $20,000 in damages.

[231] I find that the Administrator Lockdown, and the removal of Serinus' software from its IT system, disrupted the ability of Serinus and IT Ops to manage the Serinus IT environment, remotely access it to troubleshoot problems for its employees, and also disrupted Serinus' access to the database for a geology project. This situation existed for less than a week, during which almost all Serinus end-users continued to have end-user access to Serinus' systems. There is no evidence that it affected Serinus' relationships with its clients or harmed its reputation.. While there is a risk of Serinus' data being exposed and accessible by SysGen, there is no evidence that SysGen did anything with Serinus' data. Serinus managed to recover its access quickly and lock out SysGen in a few days.

[232] In the circumstances, I am not satisfied that an award of general damages is appropriate.

d. Aggravated Damages

[233] The Statement of Claim also sought aggravated damages, but this was not pursued expressly in Serinus' written argument.

[234] I do not award aggravated damages. Serinus is a corporation that has no feelings and cannot suffer an intangible injury like that which aggravated damages seeks to compensate: ***Thomas Management Limited v Alberta (Minister of Environmental Protection)***, 2006 ABCA 303 at paras 12–19; ***1234389 Alberta Ltd v 606935 Alberta Ltd***, 2020 ABQB 28 at paras 236–37; ***Inform Cycle Ltd v Draper***, 2008 ABQB 369 at para 43. Serinus cannot claim for the stress the Administrator Lockdown may have caused Mansouri personally.

[235] It may be an open question whether a corporation can claim aggravated damages if it can establish harm to its reputation, rather than hurt feelings: see e.g. ***Northwest Organics, Limited Partnership v Fandrich***, 2019 BCCA 309 at paras 126–28. I need not decide if this is possible in Alberta in this case because Serinus did not adduce any evidence of reputational damage.

2. Should Serinus be Awarded Punitive Damages?

[236] In its Statement of Claim, Serinus sought a judgment for $100,000 in punitive damages. In written argument, it refined this claim to just over $90,000.

[237] The issues are: (1) are punitive damages appropriate in this case? (2) is Serinus' punitive damages claim excluded by the 2010 Application agreement? and (3) if punitive damages are appropriate and not excluded, what is an appropriate quantum?

a. Are Punitive Damages Appropriate in this Case?

[238] Punitive damages are very much the exception, not the rule: ***Whiten v Pilot Insurance Co***, 2002 SCC 18 at para 94. They are imposed only if there has been high-handed, malicious, arbitrary or highly reprehensible misconduct that departs to a marked degree from ordinary standards of decent behaviour: ***Whiten*** at para 94; ***Jonasson v Nexen Energy ULC***, 2019 ABCA 428 at para 2. They are generally given only where the misconduct would otherwise be unpunished or where other penalties are or are likely to be inadequate to achieve the objectives of retribution, deterrence and denunciation: ***Whiten*** at para 94; ***321665 Alberta Ltd v Husky Oil Operations Ltd***, 2013 ABCA 221 at para 48. Their purpose is not to compensate the plaintiff, but to "give a defendant

his or her just desert (retribution), to deter the defendant and others from similar misconduct in the future (deterrence), and to mark the community's collective condemnation (denunciation) of what has happened": ***Whiten*** at para 94.

[239] Punitive damage awards for breach of contract are exceptional but will be awarded where the alleged breach of contract is an independent actionable wrong: ***Atlantic Lottery Corp Inc v Babstock***, 2020 SCC 19 at para 63. The actionable wrong need not be tortious; for example, punitive damages can be awarded where the defendant breaches an obligation of good faith: ***Atlantic Lottery*** at para 63.

[240] I find that SysGen's breach of contract was an independent actionable wrong. First, I have already found that the Administrator Lockdown constituted the tort of conversion.

[241] Further, a breach of a contractual obligation of good faith can be an independent actionable wrong justifying punitive damages: ***Atlantic Lottery*** at para 63; ***Whiten*** at para 79; ***Bhasin*** at para 55.

[242] Courts have also held that the duty of honest performance can constitute an independent actionable wrong: ***Bhasin*** at paras 88, 93; ***Galea v Wal-Mart Canada Corp***, 2017 ONSC 245 at para 291; ***Gordon v Altus***, 2015 ONSC 5663 at paras 39–42; ***Dengedza v Canadian Imperial Bank of Commerce***, 2021 FC 1316 at para 35; ***Atlantic Lottery*** at paras 63–66, 129–134. The duty of honest performance requires parties to be honest with each other in relation to the performance of their contractual obligations: ***Bhasin*** at para 93. I find that SysGen misled Serinus about what SysGen had done to Serinus' IT systems and why it had done it, and in doing so breached SysGen's duty of honest performance of the FSMA. That was an independent actionable wrong.

[243] Further, in ***Wastech*** the Supreme Court of Canada confirmed that a party must exercise contractual discretion in good faith. As stated by the majority, at para 88:

> In sum, then, the duty to exercise discretion in good faith will be breached where the exercise of discretion is unreasonable, in the sense that it is unconnected to the purposes for which the discretion was granted. This will notably be the case where the exercise of discretion is capricious or arbitrary in light of those purposes because that exercise has fallen outside the range of behaviour contemplated by the parties. The fact that the exercise substantially nullifies or eviscerates the fundamental contractual benefit may be relevant but is not a necessary pre-requisite to establishing a breach.

[244] In my view, a breach of the duty to exercise contractual discretion in good faith can also constitute an independent actionable wrong for the purposes of punitive damages. I find that SysGen's decision to implement the Administrative Lockdown was unreasonable in the context of the FSMA and any discretion SysGen had. SysGen's obligation was to transition services during the notice period and to continue to "maintain the security" of Serinus' IT systems without introducing new security risks. SysGen's introduction of its own security threat for the purposes of leveraging payment of disputed invoices was unconnected to the purposes for which SysGen had Administrator Access to Serinus' IT systems. This was an independent actionable wrong.

[245] It is unacceptable for an IT specialist, paid to protect the client's IT systems from security threats, to effectively hijack administrative control from their client in response to, and as a means to leverage a favourable resolution of, a billing dispute. Doing this at a time when it is known to the IT service-provider that the business functioned almost exclusively electronically and remotely was particularly egregious. In the absence of clear and enforceable contractual right, statutory or other asserted common law right authorizing the IT service-provider to do so, a party obligated or entrusted to protect another's electronic information systems could not reasonably be expected to abuse its privileged position by usurping administrative control without notice and then refusing to relinquish control until its client responds to a settlement offer. Taking steps to "gain bargaining leverage in negotiating a settlement" has been previously held to warrant the court's intervention with punitive damages: ***Fidler v Sun Life Assurance Co of Canada***, 2006 SCC 30 at para 63, citing ***702535 Ontario Inc v Non-Marine Underwriters Members of Lloyd's London,*** 2000 CanLII 5684 (ONCA), 184 DLR (4th) 687 at para 29; ***Fernandes v Penncorp Life Insurance Co***, 2014 ONCA 615 at paras 74–80.

[246] I find that SysGen's decision to implement the Administrator Lockdown, in the way it did, was high-handed and reprehensible conduct that departed to a marked degree from ordinary standards of decent behaviour.

[247] Serinus did not report the incident to the police, and there were no criminal charges pursued, so the question of whether it was a criminal act is not before me and I make no comment on that issue. However, Kayser, who I have accepted as an expert in cybersecurity, defined "cybercrime" and "computer crime" in this civil context:

> Cybercrimes are computer crimes that include some interaction or dependency on the Internet or other from of communication, such as through a wireless network, that is outside the physical domain where the targeted computer, network, or electronic device resides...

[248] Kayser defined computer crimes as:

> Computer crime occurs when a computer or other electronic media, hardware or software, or other type of electronic devices are targeted for the purposes of destruction, disruption, theft, or to commit a crime.

[249] Kayser agreed that an incident of cybercrime / computer crime could be considered a cyberattack.

[250] I find that SysGen's Administrator Lockdown targeted Serinus' IT systems to disrupt them by removing Serinus' Administrator Access through password resets, which it did remotely, to leverage its bargaining position. This conduct fit the (non-criminal) definition of cybercrime postulated by SysGen's own expert. Although not necessary to my finding that SysGen's conduct was high-handed and reprehensible conduct that departs to a marked degree from ordinary standards of decent behaviour, Kayser's definitions of cybercrime and computer crime support my conclusion. Even if not "criminal" in the legal sense, conduct that is considered computer crime in the cybersecurity industry is, in this case, conduct that is reprehensible and outside ordinary standards of decent behaviour.

[251] The expert evidence further supports my conclusion that an IT service provider cutting off administrator access to leverage a billing dispute would be outside the ordinary standards of decent behaviour. Both experts expressed what I would characterize as, at least, surprise or disbelief that an IT provider would disrupt its own client's access as part of a billing dispute. For example, Kayser's questioning included this exchange:

> Q. When you were forming your opinion, did you draw any causative link between Serinus disputing an invoice and SysGen revoking Serinus's administrator access?
>
> A. You mean were the two events correlated that I formed an opinion saying these two companies are having an issue about paying a bill and, therefore, SysGen turned and said: There, you can't have administrative access? Is that basically what you're asking me?
>
> Q. Did you explore that possibility, or did you examine that or consider that?
>
> A. No, I didn't consider that the battle got to a point if -- or whatever word you want to use. The dispute got to a point that finally somebody at SysGen said: Well, there you go. We'll just cut you off. That was not my assumption at all.
>
> Q. Okay, and you didn't explore or consider the facts in light of that being a possibility?
>
> A. I have to admit I did not approach this like two children in a sandbox having a hissy fit. That's kind of how I would characterize your question. Not being disrespectful to you, **but in business, you'd like to think that people are a little bit more mature, regardless of how angry they get. And if they're in the throes of hiring lawyers to fight a case out, it never entered my mind that all of a sudden SysGen or anybody would go: Well, I will show you. Here. Bang. That just, to me, would not be consistent with all of the preceding events that have taken place with letters back and forth between lawyers and discussions and two companies saying to each other: Look, let's get this resolved, or whatever it is, or now I have cut you off and here's your termination. It did not enter my mind that SysGen all of a sudden threw a hissy fit and cut them off**. No, it didn't. [Emphasis added]

[252] I have found, on the balance of probabilities, that SysGen did, in fact, cut off Administrator Access in response to the Billing Dispute. Kayser's evidence noted above supports my conclusion that SysGen's conduct warrants punitive damages. Further, Kayser noted that he was not aware in his entire career ever hearing of a managed service provider conducting a cyberattack against a former client. Similarly, Mansouri deposed that in a decade of being involved professionally in the IT industry, he had never seen or heard of an IT services company deliberately preventing a client or former client from having access to its own domain and servers.

[253] SysGen argues that Serinus should not be entitled to punitive damages because it does not come to the court with clean hands, relying on ***Offierski v 2253001 Ontario Inc***, 2020 ONSC 1483 at paras 73–75, which in turn cited ***BMO Nesbitt Burns Inc v Wellington West Capital Inc***, [2005] OJ No 3566 (CA), 2005 CanLII 30303 (ONCA). The plaintiff's conduct may be relevant to punitive damages where there is a causal connection between the plaintiff's conduct and the defendant's conduct in the sense that the plaintiff's conduct caused the defendant's misconduct: ***BMO Nesbitt Burns*** at para 32, citing ***TLC v Vancouver (City)***, 1995 CanLII 300 (BCSC), [1996] 2 WWR 529 at paras 95–96; ***2292772 Ont Inc v 2330829 Ont Inc***, 2017 ONSC 6415 at paras 93–96. In my view, the conduct of a plaintiff is one factor to consider by the court in determining whether punitive damages are appropriate.

[254] I find that the Serinus Dispute Letter instigated the Administrator Lockdown. And I have found that Serinus' position in the Dispute Letter was incorrect. However, these facts do not support SysGen in the way it suggests. While incorrect, Serinus' position on the interpretation of the FSMA or the FSMA Amendment was not high-handed, malicious, arbitrary or highly reprehensible. It only requested SysGen to provide the contractual reference to support SysGen's right to invoice, and that until that was provided it disputed the subject invoice. Serinus was making inquiries and advancing a legal position, as it was entitled to do, and as happens many times every day in this country. The fact Serinus was ultimately incorrect on its interpretation of the FSMA and the FSMA Amendment does not excuse SysGen's conduct or make it less offensive.

[255] I find that punitive damages are warranted against SysGen in this case.

b. Are Punitive Damages Excluded by the 2010 Application agreement?

[256] I have already found that the 2010 Application was a binding agreement on the parties at the time of the Administrator Lockdown.

[257] The 2010 Application agreement includes this provision (**Exclusion Clause**):

> In no event shall **SysGen Solutions Group, or its affiliates, or any of their respective directors, officers, employees, agents or contractors be liable for any claim for** (A) indirect, consequential or **punitive damages**; (b) damages for loss of profits or revenue, failure to realize expected savings, loss of use of Client materials, computer hardware, software, web site and any stored data; or (C) any damages whatsoever relating to third-party products or materials. In no event shall SysGen's liability to Client in respect of software or software licensing exceed the maximum value of services provided by SysGen to the Client under the services agreement. [Emphasis added]

[258] There is nothing inherently unreasonable or sinister about an exclusion clause in a freely negotiated contract: ***Dow Chemical Canada*** at para 49. Even though the 2010 Application was a SysGen form that was to be filled out by its potential clients, this alone does not make it unenforceable. Serinus did not need to accept the Exclusion Clause.

[259] The enforceability of the Exclusion Clause is governed by the principles in ***Tercon***. The court must examine (1) whether, as a matter of contractual interpretation, the clause applies to the

circumstances of the case; (2) whether the clause is invalid because it was unconscionable at the time the contract was made (as might arise from unequal bargaining power between the parties); and (3) if the clause applies and is otherwise valid, whether overriding public policy reasons nevertheless favour refusing to enforce the contractual bargain agreed to by the parties: ***Tercon*** at paras 122–23; ***Canlanka Ventures Ltd v Capital Direct Lending Corp***, 2021 ABCA 115 at para 33.

[260] I find that the first two elements of the ***Tercon*** test are met. The Exclusion Clause clearly and expressly references punitive damages and applies to Serinus' claim for punitive damages. I reject Serinus' argument that the Exclusion Clause only applies to claims related to third-party software. The paragraphs following that title are broader than that and the Exclusion Clause clearly addresses general claims beyond third-party software related claims.

[261] With respect to the second element of the ***Tercon*** test, there is also no evidentiary basis to conclude the FSMA was unconscionable at the time it was made.

[262] With respect to the third element of the ***Tercon*** test, the residual power of the court to refuse to enforce a contract on public policy grounds will rarely be exercised: ***Tercon*** at para 117. The onus is on Serinus to prove the existence of an overriding public policy that outweighs the very strong public interest in the enforcement of contracts: ***Tercon*** at para 123 (per Binnie J, dissenting but not on this point); ***Douez v Facebook, Inc***, 2017 SCC 33 at para 147 (Wagner CJ and Côté J, dissenting but not on this point); ***Owners, Strata Plan LMS 3905 v Crystal Square Parking Corp***, 2020 SCC 29 at para 23.

[263] Traditional heads of public policy (contracts in restraint of trade, injurious to the justice system, injurious to the state, affecting marriage or immoral contracts), may support the refusal to enforce an exclusion clause, but the type of public policy is not closed: ***Niedermeyer v Charlton***, 2014 BCCA 165 at para 76, citing Brandon Kain & Douglas T. Yoshida, "The Doctrine of Public Policy in Canadian Contract Law" in Todd L. Archibald & Randall Scott Echlin, eds., *Annual Review of Civil Litigation* (Toronto: Thomson Carswell, 2007) 1 at 18–28.

[264] Public policy considerations may pertain to the nature of the entire contract but may also relate directly to the nature of the breach and the conduct of the defendant: ***Tercon*** at para 117; ***Niedermeyer*** at para 79; ***Precision Drilling Canada Limited Partnership v Yangarra Resources Ltd***, 2017 ABCA 378 at para 46. The power to refuse to enforce exclusion clauses exists in the commercial context to curb abuse where a party is so contemptuous of its contractual obligations and reckless as to the consequences of its breach as to forfeit the assistance of the court: ***Tercon*** at paras 119–20, citing ***Plas-Tex Canada Ltd v Dow Chemical of Canada Ltd***, 2004 ABCA 309.

[265] Although it is clear that, in practice, commercial parties often attempt to exclude liability for punitive damages in their contracts (as just one example, see ***Dow Chemical Canada*** at para 44), the parties did not point me to any jurisprudence specifically assessing whether there is an overriding public policy reason to refuse to enforce an exclusion for liability for punitive damages.

[266] There are some types of claims, obligations or remedies where overriding public policy concerns trump private parties' ability to limit their obligations or liability. For example, the duty of honest performance cannot be excluded by the parties: ***Bhasin*** at para 75; ***Canlanka*** at para 27. Liability for fraudulent conduct cannot be excluded: ***Roy v Kretschmer***, 2014 BCCA 429 at para

75; ***Chua v Van Pelt***, 1977 CanLII 298 (BCSC), 74 DLR(3d) 244 at para 29, citing ***Ballard v Gaskill***, 14 WWR 519, [1955] 2 DLR 219 (BCCA).

[267] I find that, for public policy reasons, the remedy of punitive damages cannot be excluded by contract, although an attempt to exclude it may be a factor relevant in determining whether punitive damages are appropriate or in determining the quantum of any punitive damages award.

[268] This conclusion is consistent with the unique nature of punitive damages. As confirmed by the Supreme Court of Canada, they are not compensatory, but are for the purposes of retribution, deterrence and denunciation and, therefore, straddle the frontier between civil law (compensation) and criminal law (punishment): ***Whiten*** at paras 36, 44, 94; ***Nevsun*** at para 221 (Brown and Rowe JJ dissenting in part). They are awarded against misconduct that "offends the court's sense of decency": ***Hill v Church of Scientology of Toronto***, 1995 CanLII 59 (SCC), [1995] 2 SCR 1130 at para 196; ***Whiten*** at para 36. As such, in my view, punitive damages engage the court's public role in the proper administration of our justice system in a way that goes beyond settling the compensatory claims between private parties.

[269] Where it has been found that a party has engaged in conduct that warrants punitive damages, it is open for courts to refuse to enforce exclusion clauses which attempt to privately oust the jurisdiction of the court to supervise and punish commercial behaviour that is outside the court's sense of decency. Contracting parties should never feel that they will invariably be able to hide behind exclusion clauses if their conduct is high-handed, malicious, arbitrary or highly reprehensible.

[270] In this case, given the context and nature of SysGen's conduct, I find that it would be against public policy to allow SysGen's conduct to go unpunished. SysGen abused its access to Serinus' systems, inserted a security risk which required Serinus to have to engage in what SysGen's expert states was a highly risky effort to regain Administrator Access to its own systems, and disrupted the transition of services SysGen agreed and undertook to facilitate. All of this showed a contempt for SysGen's contractual obligations and a recklessness to the consequences such that it forfeited the court's assistance.

[271] I do not enforce the Exclusion Clause.

c. What is an Appropriate Quantum of Punitive Damages?

[272] Punitive damages should be awarded in an amount that is no greater than necessary to rationally accomplish their purpose of retribution, deterrence and denunciation, and should be assessed in an amount reasonably proportionate to such factors as the harm caused, the degree of misconduct, the relative vulnerability of the plaintiff and any advantage or profit gained by the defendant: ***Whiten*** at para 94; ***1007374 Alberta Ltd v Ruggieri***, 2015 ABCA 205 at para 13; ***Breen*** at para 540.

[273] In ***Luft v Taylor, Zinkhofer & Conway***, 2017 ABCA 228 at para 58, the Court of Appeal has most recently set out these factors as instructive when determining a proportionate award:

(a) the blameworthiness of the defendant's conduct;

(b) the vulnerability of the plaintiff;

(c) the harm or potential harm directed specifically at the plaintiff;

(d) the need for deterrence;

(e) civil and criminal penalties which have been or are likely to be inflicted on the defendant for the same misconduct; and

(f) the advantage wrongfully gained by a defendant from the misconduct.

[274] I address the relevant factors below.

i. Blameworthiness of the Defendant's Conduct

[275] The level of blameworthiness of the defendant may be influenced by a number of factors, but in ***Whiten*** the Supreme Court of Canada noted these factors: (1) whether the misconduct was planned and deliberate; (2) the intent and motive of the defendant; (3) whether the defendant persisted in the outrageous conduct over a lengthy period of time; (4) whether the defendant concealed or attempted to cover up its misconduct; (5) the defendant's awareness that what he or she was doing was wrong; (6) whether the defendant profited from the misconduct; (7) whether the interest violated by the misconduct was known to be deeply personal to the plaintiff or a thing that was irreplaceable: ***Whiten*** at para 113.

[276] In oral argument, SysGen put its own conduct into some relevant context:

> At the time of the password reset, the end of the FSMA was imminent. SysGen was concerned it would be held responsible for the IT systems after it formally handed over [Managed Service Provider] responsibility. It took what I would characterize as a misguided step based on those concerns. SysGen certainly could have done things differently. It delayed in reacting to the security issues it was responding to by about a month. It did not follow best practices in the way that it reset administrative passwords. It should have discussed what it was doing with Serinus sooner and more clearly and the reasons and what its plans were. And in general the communications by both SysGen and Serinus during this critical period in April 2020 were strained and should have been better.

[277] This was a frank acknowledgement about SysGen's conduct in some respects, but then SysGen went on to deny any evidence of malicious intent.

[278] In my view, even if it is accepted that SysGen did not have malicious intent, its conduct was blameworthy and was not a measured response as argued by SysGen's counsel.

[279] The Administrative Lockdown, and the deletion of Serinus' software from its system, was a deliberate attempt to leverage SysGen's bargaining position in the Billing Dispute, at the very end of the notice period designed to transition services away from SysGen. SysGen effectively held administrative control over Serinus' system hostage over the weekend to heighten that leverage, even though (on its own evidence) it had already decided to (but not informed Serinus that it was going to) end the relationship and presumably return Administrator Access to Serinus.

The conduct was short-term and lasted over only a few days. However, it is unknown exactly how long the situation would have lasted had Serinus not been able to conduct the Serinus Restoration. The decision to implement the Administrator Lockdown was not documented under SysGen's existing policies or at all. SysGen's responses to Serinus' questions were vague and misleading. Based on SysGen's evidence, it does not appear that Richardet and Jordan properly appreciated that the conduct was wrongful. SysGen's attempt to achieve bargaining leverage back-fired and it has had to engage in this lengthy litigation. Serinus' impacted IT system was not deeply personal, but it was irreplaceable in the sense that Serinus needed Administrator Access to administer its IT system.

ii. The Vulnerability of the Plaintiff

[280] The financial or other vulnerability of the plaintiff, and the consequent abuse of power by a defendant, is highly relevant where there is a power imbalance: ***Whiten*** at para 114. This factor militates against an award of punitive damages in most commercial situations, because most participants enter the marketplace knowing it is fuelled by the aggressive pursuit of self-interest: ***Whiten*** at para 115. Courts must watch and ensure that there is not double recovery for the same vulnerability both under aggravated or general damages and punitive damages, because punitive damages are not compensatory: ***Whiten*** at para 116.

[281] The security of Serinus' IT system was vulnerable to SysGen. On the other hand, as I have found earlier, Serinus was not peculiarly vulnerable to SysGen sufficient to create an *ad hoc* fiduciary relationship. It was a sophisticated organization being assisted by IT Ops and could have taken more steps to protect itself from SysGen following the Termination Letter and before the Administrator Lockdown.

iii. The Harm or Potential Harm Directed Specifically at the Plaintiff

[282] It would be irrational to provide Serinus with an excessive windfall but, on the other hand, malicious and high-handed conduct which could be expected to cause severe injury is not necessarily excused because fortuitously it results in little damage: ***Whiten*** at para 117.

[283] The harm actually experienced as a result of SysGen's conduct ended up being modest. However, the risk of harm was more significant given the loss of Administrator Access. Had something significant happened to Serinus' IT system during the days it had no control, and while SysGen was in control but obfuscating what it was doing, the impact could have been much worse. Further, Serinus reasonably made the decision to implement the Serinus Restoration, which according to SysGen was a risky operation. Therefore, SysGen put Serinus in the position of having to decide whether to capitulate to SysGen's offer or to put its system at risk to regain control. A punitive damages award must take into account the significant risk that SysGen introduced which is not reflected in the relatively minor compensatory damages award.

iv. The Need for Deterrence

[284] Deterrence is an important justification for punitive damages: ***Whiten*** at para 120. It may play an even greater role if the conduct is a typical approach of a defendant: ***Whiten*** at para 120.

[285] I find that the need for deterrence in this case is high. As our society and business community relies increasingly on electronic information and databases, a clear message must be sent to those having privileged access to others' information systems, that they cannot use that privileged access against the owner of the information systems to resolve business disputes that may arise, unless that power is made clear in enforceable contractual provisions that are brought to the attention of their clients, applicable statutory provisions, or other clearly claimed and applicable common law rights.

[286] If conduct like SysGen's in this case is not deterred, many parties faced with a similar situation, where amounts in dispute may be small, will be incentivized to simply capitulate on the dispute, or pay a ransom, to avoid the cost and inconvenience of challenging the conduct.

[287] Further, in this case, Richardet boasted in his questioning about how effective his collection efforts are and admitted that he had restricted administrator access to SysGen's customers several times. SysGen's apparent practice of treating its clients this way, without clear contractual, statutory or claimed common law rights to do so, must be deterred and denounced.

[288] An appropriate punitive damages award will hopefully motivate better behaviour in the future. I reject SysGen's suggestion that it has been sufficiently punished by having to defend this action.

v. Other Penalties

[289] I am not aware of any other penalties in this case.

vi. Other Advantages

[290] A traditional function of punitive damages is to ensure that the defendant does not treat compensatory damages merely as a licence to get its way irrespective of the legal or other rights of the plaintiff: ***Whiten*** at para 124.

[291] I am not aware of any other advantages SysGen obtained. I suspect that it regrets its decision to implement the Administrator Lockdown over a billing dispute.

vii. Conclusion re Punitive Damages

[292] Based on my review of the above factors, and taking into account my findings in this matter, I find that a punitive damages award in the amount of $50,000 is appropriate and proportionately meets the requirements of retribution, deterrence and denunciation.

3. Conclusion re Serinus' Damages

[293] Serinus is entitled to judgment in the aggregate amount of $97,012.50, as below:

Item	Amount ($)
Personnel Costs	5,000.00
Amounts Paid to iON	42,012.50
Punitive Damages	50,000.00
TOTAL	97,012.50

H. Is Serinus Liable to SysGen on the Counterclaim?

[294] SysGen's Counterclaim includes claims for unpaid FSMA Services, unpaid Data Storage Services, damages respecting the Data Storage Services in the form of what it refers to as the "Three Year Agreement", and for unpaid Software Licencing Services. SysGen relies on the terms of the 2010 Application, the FSMA Agreement, and purchase orders to support its claim. It also claims unjust enrichment in the alternative. Serinus defended the Counterclaim on the basis that no amounts were owed or payable to SysGen.

[295] I address the effect of the 2010 Application as a threshold question before addressing the different categories of claim in the Counterclaim.

1. What is the Legal Effect of the 2010 Application?

[296] I have earlier found that the 2010 Application was a binding contract that continued to be active in 2020. In support of its Counterclaim, SysGen argues that Serinus was required to pay for materials and services supplied within 15 days of the issuance of an invoice and that any dispute of an invoice must be made within 7 days of its issuance.

[297] I disagree that the 2010 Application has the effect as asserted by SysGen.

[298] First, it is the credit terms of SysGen's invoices, which are the subject of its Counterclaim, which govern if they are different than the credit terms in the 2010 Application agreement. SysGen cannot rely on the 2010 Application to say that the invoices had to be paid on more stringent credit terms. In any event, the credit terms don't affect whether SysGen had the substantive right to issue or be paid for the invoice.

[299] Second, SysGen's argument that Serinus is deemed to have accepted SysGen invoices overstates the 2010 Application's Terms and Conditions about disputing invoices. The 2010 Application's Terms and Conditions only provide that "I understand that if there is an issue with an invoice, reasonable attempts to clarify the issue should be made within seven (7) days of receipt of the invoice." In my view, this does not affect the question of whether SysGen is substantively entitled to payment for its invoices – it is not a deeming provision. Even if it is accepted that Serinus did not make reasonable attempts to clarify invoices within this timeframe, SysGen has not established any damages arising from that.

[300] I now turn to SysGen's specific claims in its Counterclaim.

2. Is Serinus Liable for Unpaid FSMA Services?

[301] SysGen claims an aggregate amount of $19,380.90 for unpaid FSMA Services.

[302] I have found that the Termination Letter properly provided 90-day's notice of the termination of the FSMA, which would be effective at the end of April 2020 such that, as of May 1, 2020, the FSMA would be at an end. Based on this, unless SysGen breached or repudiated the FSMA, it was entitled to be paid the $9,000 monthly fee pursuant to the FSMA Amendment. SysGen's position is that it continued to provide FSMA services until it was locked out following the Serinus Restoration and is entitled to be paid.

a. February 2020 FSMA Services

[303] On January 31, 2020, SysGen invoiced Serinus in advance for February 2020 FSMA services (Invoice ADV-39769), Yaniw approved it, and Serinus paid it on March 24, 2020.

[304] Serinus' position respecting FSMA Services for February 2020 is inconsistent. Even though Serinus approved and paid the invoice in March, in the April 20, 2020 Dispute Letter, Serinus questioned the contractual basis for it — and this led to the Administrator Lockdown. Then, Serinus strengthened its position on April 23, 2020 and disputed SysGen's entitlement to be paid for the invoice at all. In their affidavits, Auld and Yaniw state that the invoice was paid in error. However, Serinus never included recovery of this paid invoice in its Statement of Claim. Then, in its written argument, it appeared to take a new position that SysGen was entitled to charge for FSMA Services for the month of February because the FSMA required 30 days' or one-month's notice.

[305] Ultimately, as the February 2020 invoice for FSMA Services was paid, is not the subject of the Counterclaim, and Serinus does not claim it should be repaid, I make no findings about it.

b. March 2020 FSMA Services

[306] Serinus argues that SysGen is not entitled to charge for FSMA Services in March or April 2020 because the 30-day-notice period had expired. This position is rejected as I have found that the FSMA continued during the 90-day notice period.

[307] I find, on the balance of probabilities, that SysGen continued to provide on-site support until March 15, 2020 when Serinus closed its offices due to COVID. Further, Serinus acknowledges that SysGen continued to answer Serinus service requests in March, even though Serinus now had IT Ops involved and Mansouri and IT Ops were handling a lot of service requests themselves. Several requests were from Yaniw who was in senior management at Serinus. In my view, this evidence is consistent with the concept embedded in the FSMA that during the notice period there would be a transition period where the FSMA Services would diminish over time until the end of the notice period. In my view, all else being equal, the reduced level of FSMA Services does not change SysGen's entitlement to its flat monthly fee.

[308] Serinus also argues that SysGen should only be entitled to charge time and materials for March FSMA Services, because the Termination Letter provides for that. I disagree. The Termination Letter did not create contractual obligations beyond the FSMA, and further, it only stated that "if SysGen is required to remedy *any issues outside of our normal FSMA agreement*" (emphasis added), then these hours would be billed at $160 per hour.

[309] Elsewhere in its argument, Serinus alleges that SysGen breached the FSMA for failing to discharge what Serinus refers to as the "Asset Management Obligation". On March 4 2020, Serinus wrote to SysGen repeating an earlier request for access details for Microsoft that had not been provided. Serinus also noted that SysGen did not appear to have a discrete set of documentation or any handover documentation to assist Serinus in its transition of services from SysGen. Serinus repeated its request for the missing Microsoft details, but SysGen did not respond. This took place around the same time in early March when SysGen was well aware that Serinus had retained a new IT service provider. Serinus did not claim or prove its damages for these alleged breaches of the FSMA.

[310] Serinus also argues that SysGen repudiated the FSMA through the Administrator Lockdown. I agree that it did, however, a repudiation does not extinguish the rights and obligations that have already matured: ***Guarantee Co*** at para 40; ***Booster Juice Inc v West Edmonton Mall Property Inc***, 2019 ABCA 58 at para 19. I will address repudiation further in respect of the April FSMA Services.

[311] I find that, in the circumstances, SysGen was entitled to be paid its $9,000 monthly fee (plus tax) pursuant to the FSMA for the month of March 2020. It is entitled to $9,690.45.

c. April 2020 FSMA Services

[312] SysGen breached the FSMA by failing to remove its RMM Software in early April 2020 as requested (and after it confirmed it would). SysGen then repudiated the FSMA on April 21, 2020 through the Administrator Lockdown.

[313] I find that, even though Serinus was not 100% sure at the time that SysGen was responsible for the Administrator Lockdown, Serinus actually believed in fact that SysGen was responsible, and Serinus communicated its acceptance of SysGen's repudiation and terminated the FSMA by sending the April 24, 2020 letter, regaining control of its own IT systems over the weekend and locking SysGen out of its systems. Therefore, the FSMA terminated on or about April 26, 2020 and the parties were discharged from future obligations: ***Guarantee Co*** at para 40; ***Booster Juice*** at para 19.

[314] In the circumstances, SysGen is not entitled to be paid for any FSMA Services it may have provided in the month of April 2020, including because it breached and repudiated the FSMA, Serinus accepted the repudiation, and the FSMA terminated before SysGen's right to be paid its monthly fee had accrued.

3. Is Serinus Liable for Unpaid Data Storage Services?

[315] SysGen claims a collective amount of $10,466.83 for unpaid Data Storage Services.

[316] SysGen's claim relates to three different storage devices and is based on three purchase orders — a December 15, 2016 purchase order, a November 20, 2017 purchase order and a May 2018 purchase order (**PO 87**). These purchase orders all make it clear that there was an initial charge and then a monthly recurring fee. It is express or implied that as long as the Data Storage Services were being used, then the monthly fee applied.

[317] In the Termination Letter, SysGen confirmed that it would continue to provide and bill for the Data Storage Services, and Serinus did not respond to that letter.

[318] Serinus acknowledges some of the Data Storage Services invoices, but states that they should be adjusted due to breaches of the "Asset Management Obligation" under the FSMA. However, Serinus did not include those claims in its Statement of Claim and did not seek set-off in its Statement of Defence to the Counterclaim. Further, it did not quantify any alleged damages for breach of the Asset Management Obligation.

[319] Serinus also argues that SysGen repudiated the Data Storage Services agreements or purchase orders. I agree that the Administrator Lockdown was also a repudiation of the agreement respecting the Data Storage Services, since charges for the Data Storage Services were part of invoice ADV-39126 which were subject of the Dispute Letter and which led to the Administrator Lockdown. However, unlike with respect to the FSMA, Serinus did not accept the repudiation but rather affirmed the existing Data Storage Services by seeking quotes for a reduction in the Data Storage Services retention plan on April 27, 2020, and then continuing to use the data storage devices until June 2020. There is no evidence Serinus attempted to terminate those services or return the devices before that. SysGen is entitled to be paid the agreed Data Storage Services monthly fees. Serinus was not entitled to use the devices or receive storage services for free. SysGen is entitled to $10,466.83 as claimed.

[320] SysGen also alleges that, with respect to PO 87, Serinus agreed to a three-year term for that particular storage device in return for a discounted up-front price for the device. SysGen argues that it has lost the benefit of 11 months of the term (July 2020 to May 2021). It claims $4,709.54 in lost profits for the remaining term based on the $1,427.14 per month it would have received from Serinus minus the $999 it had to pay to the device supplier. I find that, on the balance of probabilities, PO 87 reflects an agreement that Serinus would receive a reduced initial price in return for committing to 3 years of Data Storage Services in respect of the subject storage device. SysGen is entitled to an additional $4,709.54 in respect of PO 87 as damages for lost profits.

[321] Accordingly, SysGen is entitled to $15,176.37 in respect of Data Storage Services.

4. Is Serinus Liable for Unpaid Software Licencing Services?

[322] SysGen claims for Software Licencing Services from February to June 2020 in the aggregate amount of $28,271.07.

[323] In the Termination Letter, SysGen confirmed that it would continue to provide and bill for the Software Licencing Services. Serinus did not respond to that letter.

[324] Serinus acknowledges some of the Software Licencing Services invoices, but again states that they should be adjusted due to breaches of the "Asset Management Obligation" under the FSMA. This argument is rejected for the same reasons as for the Data Storage Services.

[325] Further, like the Data Storage Services, it is express or implied in the agreement reflected in the Software Licencing Services purchase order that, as long as Serinus used the Software Licensing Services, the monthly fee applied. As the Software Licensing Services charges were not part of the Dispute Letter, it cannot be said that the Administrator Lockdown was a repudiation of

the parties' agreement respecting the Software Licensing Services. In any event, even if there was a repudiation, it was not accepted by Serinus but rather Serinus affirmed the agreement by continuing to use the software licences until June 2020.

[326] SysGen is entitled to $28,271.07 for the Software Licensing Services.

5. Conclusion re SysGen Counterclaim

[327] Given my findings, I need not address SysGen's unjust enrichment claim.

[328] In conclusion, SysGen is entitled to judgment in the aggregate principal amount of $53,137.89, as set out below:

FSMA Services	9,690.45
Data Storage Services	15,176.37
Software Licencing Services	28,271.07
Total	53,137.89

VII. Conclusion

[329] In conclusion, Serinus is entitled to judgment in the amount of $97,012.50 and SysGen is entitled to judgment in the amount of $53,137.89. I set these amounts off against each other and award Serinus judgment against SysGen in the net amount of $43,874.61 plus pre-judgment interest from June 1, 2020 to the date of this judgment, and post-judgment interest to the date of payment.

[330] The parties have had mixed success in this matter, and I suspect both will find their respective victories to be rather pyrrhic given the obvious expense they have incurred to litigate this matter to its conclusion. Accordingly, the parties are strongly encouraged to reach a resolution on costs.

[331] In the event the parties are unable to reach agreement on costs of this action, the following process shall apply:

(a) within 30 days of this decision, each party shall file and serve on the opposing party and submit to my office a written cost submission setting out their costs position. Each party's costs submission shall provide: (a) their position with respect to the factors set out in rule 10.33; (b) any formal offer or other settlement offer they wish considered; (c) a draft proposed bill of costs pursuant to Schedule C of the *Rules*; (d) a summary of their proposed reasonable and proper costs that the party incurred in respect of the action. These submissions will be a maximum of 3 pages in letter format, single spaced (excluding authorities, offers, proposed bills of costs), and

(b) within 60 days of this decision, each party shall file and serve on the opposing party and submit to my office their response submission to the other party's cost submission, to a maximum of 3 pages in letter format, single spaced (excluding authorities).

[332] If no submissions are received pursuant to this direction, there shall be no order as to costs.

Heard on the 2nd and 3rd days of March, 2023.
Dated at the City of Calgary, Alberta this 7th day of November 2023.

M.A. Marion
J.C.K.B.A.

Appearances:

Jordan Bierkos and Mark J. Risebrough
for the Plaintiff/Defendant by Counterclaim

Blake Hafso
for the Defendant/Plaintiff by Counterclaim