

# Saskatchewan Land Surveyors Association Cyber and Privacy Liability

December 2020

---

Mark Sampson, Arthur J. Gallagher Canada Limited



Insurance | Risk Management | Consulting

# AGENDA

---

## 1. Introduction

- Professional Liability Insurance Committee

## 2. Cyber and Privacy Liability

- Common Terms
- Cyber Liability Claim Statistics – Chubb Insurance
- Canada's New Digital Privacy Act
- Recent Canadian Claim Examples
- Suggestions how to Avoid a Data Breach
- Suggestions how to Combat Social Engineering Fraud
- Cyber and Privacy Liability Insurance Program
  - For the members of PSC

# PSC – Professional Liability Insurance Committee

---

## PLIC Contacts:

- Dave Gurnsey, Chair – Saskatchewan
- Mitch Ettinger – Alberta
- Michael Kidston – British Columbia
- Derik DeWolfe – Nova Scotia
- Derek French – PEI
- Daren Patkau – PSC Board Representative

What image to you think of when you hear the terms:

---

**“Cyber Attack”**

**“Social Engineering”**

**“Phishing”**







# Privacy Liability – 10 Years Ago



# Privacy and Cyber Liability - today

---





# Cyber and Privacy Liability

## Common Terms

- **Cyber Liability**

- The legal responsibility for "cyber" assets, which might include email, websites, customer or employee information, and any other data or material stored digitally (on the cloud, on a machine's hard drive, or on external storage devices).



# Cyber and Privacy Liability

## Common Terms

---

- **Privacy Injury / Liability**

- A privacy injury is caused by the company's failure to properly manage private information such as corporate confidential information of a third party.
- This can include breach of privacy laws and an unintentional breach of the company's privacy policy.



# Cyber and Privacy Liability

## Common Terms



- **Data Breach**

- A data breach is an incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner.
- It is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.
- Stolen data may include credit card numbers, customer data, trade secrets, or employee data.
- **It takes 173 days on average to identify a data breach**

# Cyber and Privacy Liability

## Common Terms

- **Social Engineering**

- The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.



# Cyber and Privacy Liability

## Common Terms

---

- **Phishing**

- Is a form of Social Engineering
- The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.





# Cyber and Privacy Liability

## Common Terms

---

- **Malware**

- Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.



# Cyber and Privacy Liability

## Common Terms

---

- **Ransomware**

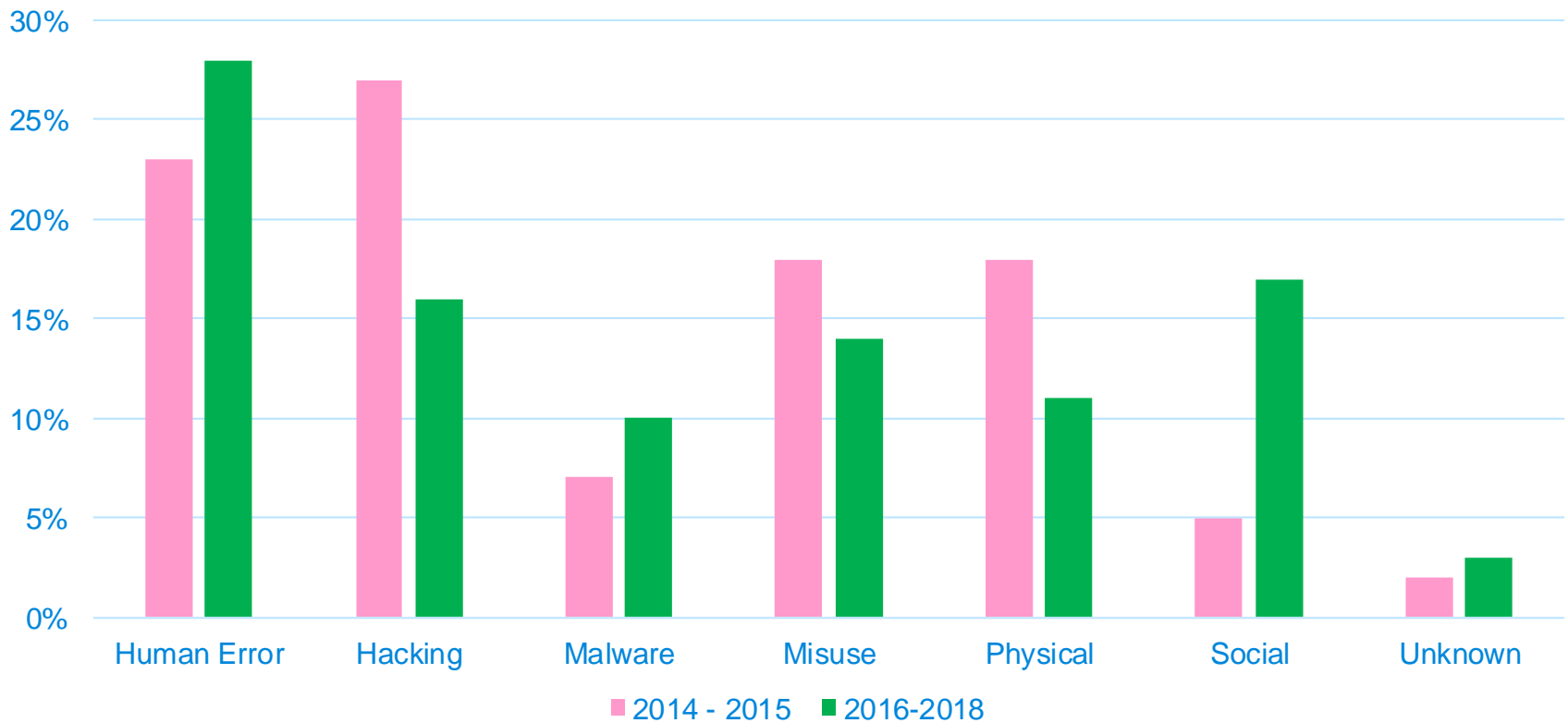
- a type of malicious software designed to block access to a computer system until a sum of money is paid.



# Chubb Insurance Company

## Cyber Liability Claim Statistics – 2014-2018

% of Claim Count by Action



# Canada's Digital Privacy Act

## Changes – November 1, 2018

---

- Federal Digital Privacy Act
- Bill S4, update to PIPEDA providing for mandatory breach notification and penalties for failure to notify.
- Notification under Federal law required when there is a 'real risk of significant harm' to the individual
- Visit the Office of Privacy Commissioner of Canada for more changes and comprehensive information on the changes to the Digital Privacy Act.

# Recent Canadian Cyber Claims

---

- **Town of Wasaga Beach**

- Ransomware – malicious software was contracted that blocked all 11 of their servers.
- Scammers originally demanded 11 Bitcoins (\$144,000 at the time) to release the servers.
- After 7 weeks of negotiation, the Town agreed to pay 3 Bitcoins (\$35,000) to release 4 servers that contained the vast majority of the town's data.
- It would have cost +\$200,000 to rebuild/recreate all their data/system from scratch.



# Recent Canadian Cyber Claims

---

- **Town of Wasaga Beach**

- Factoring payments to consultants, experts, overtime and lost productivity costs, the Town estimated the total cost of the hack is +\$300,000.
- The Town had to use its reserve fund to pay for the costs.
- Details such as how the attack occurred, and recommendations related to preventing future attacks, were redacted from the public report.
- The town has since updated its antivirus protection and invested in an new email security solution to reduce exposure to phishing and spam emails.

# Recent Canadian Cyber Claims

---

- **CarePartners**

- Provides home medical care services on behalf of the Ontario government.
- The names and contact information of thousands of patients, as well as detailed medical records and health card numbers, were obtained by cybercriminals.
- It is alleged that the employee information stolen included T4 tax slips, social insurance numbers, bank account details and plaintext passwords.

# Recent Canadian Cyber Claims

---

- **CarePartners**

- The attackers told CBC News in an encrypted message that they discovered vulnerable software on CarePartners' network that had not been updated in two years "by chance"
- They were able to exploit those vulnerabilities and weak passwords to remove hundreds of gigabytes "completely unnoticed."

# Recent Canadian Cyber Claims

---

- **CarePartners**

- The company says its forensic investigation has so far identified 627 patient files and 886 employee records that were accessed.
- Hacking Group called “OrangeWorm” has threatened to release the data without payment of Bitcoins.

# Recent Canadian Cyber Claims

---

- **Ontario 407 Private Freeway**
  - Employee theft of 60,000 records.
  - Investigation ongoing.
  - <https://globalnews.ca/video/4216520/nh-sos-407-data-breach-oshea-may-17>



# Recent Cyber Claims

---

- **Alaska Municipality**

- Anchorage metropolitan area.
- 500 desktop computers, 120 servers were infected and held hostage to ransomware.
- Also affected door entry card system and network back-ups.
- Believed malware may have entered the system in May 2018 but spread on July 24<sup>th</sup>2018.
- Staff had to use typewriters and hand written receipts (*“a typewriter is a machine that allows a person to print words directly onto paper without a computer”*)

# Recent Cyber Claims

---

- **Marriott International – Nov. 30, 2018**
  - Starwood guest reservation database hacked.
  - 500 million guests information may have been stolen
    - Name, address, phone #, passport number, date of birth, gender, credit card numbers
  - Upon investigation, Marriott discovered that the unauthorized access began in 2014.

# Recent Canadian Cyber Claims

---

- **Western Canada Survey Firm**
  - Ransomware
  - Locked system and Back-up Systems
  
- **Ontario Survey Firm**
  - Ransomware event
  - No insurance coverage

# Suggestions on how to Avoid a Data Breach Event



# Suggestions on how to Avoid a Data Breach Event

---

- Consult an Expert!
- Security Vulnerability Assessment
  - Conducted by a 3<sup>rd</sup> Party
- Employee Training
  - Not all privacy breaches are driven by criminals. More than 1/3<sup>rd</sup> of all breaches are either intentionally or accidentally caused by employees.
- Incident Response Plan

# Social Engineering – “Human Hacking”



# Social Engineering – “Human Hacking”

---

- Some criminals consider it much easier to abuse a person’s trust than to use technical means to hack into a secured computer system:
  - Trick targets into giving them information by exploiting certain qualities in human nature.
  - Use various forms of communication, such as email, Internet, or by telephone.
  - Humans tend to be the “weakest link” in the security chain.



# Social Engineering – “Human Hacking”

---

- Sample Tactics:
  - **Impersonation:**
    - A person in authority, a fellow employee, IT representative, or vendor in order to gather confidential or other sensitive information.
  - **Phishing and Spear-Phishing:**
    - Phone call or email from someone claiming to be in a position of authority who asks for confidential information, such as a password.
    - Can also include sending emails to organizational contacts that contain malware designed to compromise computer systems or capture personal or private credentials.

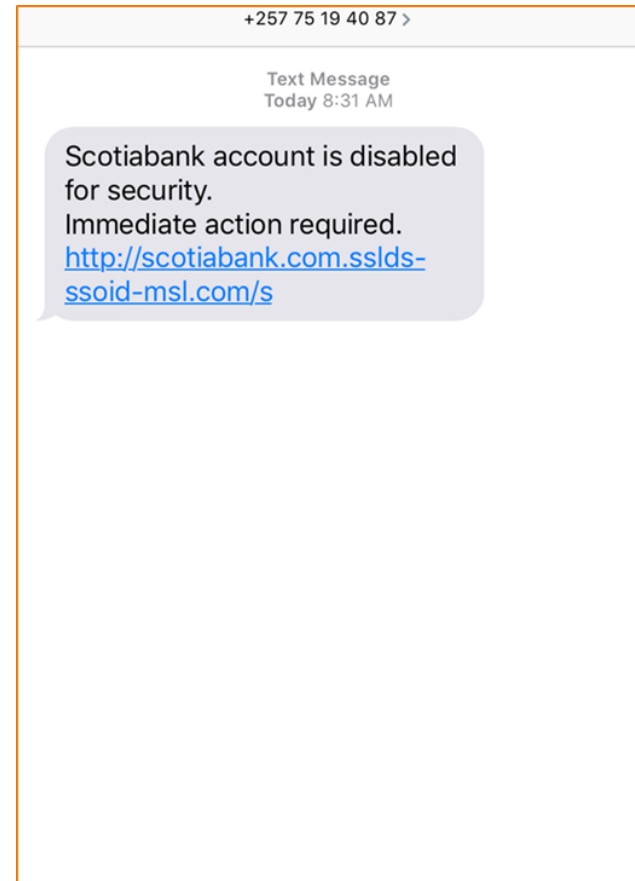
# Social Engineering – “Human Hacking”

---

- Sample Tactics:
  - **Trash cover/forensic recovery:**
    - Attackers collect information from discarded materials such as old computer equipment (hard drives, thumb drives, CDs, photocopiers) and company documents that were not disposed of securely (shredded documents).
  - **Baiting:**
    - Leaving an innocent-looking, malware-infected device - such as a USB drive, CD or DVD - at a location where an employee will come across it, and then out of curiosity will plug/load the infected device into his or her computer.

# Social Engineering - examples

- I received this text on my phone



# Social Engineering - examples



# Social Engineering - examples

- Manufacturer
  - Key Supplier
  - Change of Banking Information
- Survey Firm
  - iTunes Gift Cards



# Suggestions on how to combat Social Engineering Fraud

- Awareness through corporate culture, education and training.
  - It is not enough for a workforce to simply follow a policy guideline.
  - Employees must be educated on how to recognize and respond to an attacker's methods and thus become a "human firewall."
  - Train staff to recognize psychological methods that social engineers use: power, authority, enticement, speed and pressure. *"If it is important enough to move quickly on, it's important enough to verify"*
  - Internal training and "testing" employees.

# Suggestions on how to combat Social Engineering Fraud

---

- **Conduct a data classification assessment**
  - Identifying which employees have access to what types and levels of sensitive company information.
  - Know who the primary targets of a social engineering scheme are likely to be.
  - Remember, all employees are at risk.



# Suggestions on how to combat Social Engineering Fraud

---

- Never release confidential or sensitive information to someone you don't know or who doesn't have a valid reason for having it.
  - Even if the person identifies himself or herself as a co-worker, superior or IT representative.
  - If a password must be shared, it should never be given out either over the phone or by email.
  - **Personal Example – Gallagher IT Department**

# Suggestions on how to combat Social Engineering Fraud

---

- **Physical documents and other tangible material**
  - Documents should be shredded and computer hardware/software should be destroyed prior to disposal.
- **Guard against unauthorized physical access**
  - Maintain strict policies on displaying security badges and other credentials and making sure all guests are escorted.
  - Politely refuse entry to anyone “tailgating.”
  - Keep sensitive areas, such as server rooms, phone closets, mail rooms and executive offices, secured at all times.

# Suggestions on how to combat Social Engineering Fraud

---

- **Establish Internal Procedures:**
  - Verify incoming cheques, ensure clearance prior to transferring any money by wire.
  - Establish call-back procedures to clients and vendors for all outgoing fund transfers to a previously established phone number.
  - Implement a customer verification system with similar dual verification properties.
  - Verify any changes to customer or vendor details, independent of the requester of the change

# Suggestions on how to combat Social Engineering Fraud

---

- Be suspicious of unsolicited emails and only open ones from trusted sources.
  - Never forward, respond to or access attachments or links in such emails; delete or quarantine them.
  - Watch out for misspellings, or generic information included in an email
  - Scams usually request urgent or immediate action.
  - Scams convey dire consequences if you fail to respond.
  - Scams provide links to click within the e-mail. You can view the true destination for the link by holding your pointer over the URL.

# Suggestions on how to combat Social Engineering Fraud

**From:** Bank of America <crvdqi@comcast.net>  
**Subject:** Notification Irregular Activity  
**Date:** September 23, 2014 3:44:42 PM PDT  
**To:** Undisclosed recipients: ;  
**Reply-To:** crvdqi@comcast.net



## Online Banking Alert

Would be capitalized

**Dear member:**

We detected unusual activity on your Bank of America debit card on **09/22/2014**. For your protection, please verify this activity so you can continue making debit card transactions without interruption.

**Please sign in to** your account at <https://www.bankofamerica.com>

to review and verify your account activity, After verifying your debit card transactions we will take the necessary steps to protect your account from fraud.

<http://bit.do/ghsdfhgsd>

If you do not contact us, certain limitations may be placed on your debit card.

Grammatical Error

© 2014 Bank of America Corporation. All rights reserved.

# Preventing Phishing

Great news! You get to represent our organization at the upcoming conference in London!

Click an online post to see how this information may be exploited by a spear phisher.



**Sampson, Mark** is traveling to London, UK

Monday, August 07

On the way to London!



**Sampson, Mark** is at the Big Conference in London, UK

Wednesday, August 09

Wow, lots of great panelists and booths on the showroom floor. Great to meet more professionals in the industry.



**Sampson, Mark**

Wednesday, August 09

Anyone know of any good pubs near Paternoster Square?





### Example Spear Phishing Message

**An Issue With Your Hotel Reservation**  
From: donotreply@hotelnotifier.co  
To: Sampson,Mark

Dear Sampson,Mark, we've detected a payment issue with your reservation for



Reservation:	1 Queen Bed Room No smoking; 1 Queen Bed Non Smoking
Stays:	1 Room(s), 3 Night(s)
Occupancy:	1 Adult(s), 0 Children 0-17
Check in:	Tuesday, 08/09 After 2:00 PM
Check Out:	Friday, 08/12 Before 11:00 AM

<http://200.181.57.130/n/websec-cmd#login/index.php>

Please [click here](#) to contact our service desk and resolve the issue.

**YOUR RESERVATION WILL BE CANCELED IF YOU DO NOT RESPOND BEFORE MONDAY 8/8 6PM.**

Thank you,  
TravelPro Reservation Team



Even innocent sounding posts can give spear phishers the information they need to craft customized messages. Remember that what you do online is often public, so be sure to minimize the amount of work-related information you share. Click **SHOW ME MORE** to see other spear phishing examples.

**SHOW ME MORE**




### Example Spear Phishing Message

#### Resume

From: Jaqueline Canton (lima@limator.com.tr)

To: Sampson,Mark

Attachment:  Resume\_v2.PDF

Dear Sampson,Mark,

Many warm regards and thanks for speaking with me at the Big Conference. Maybe you don't remember me ... but I was there when you shared details about your company's vision for the coming year. I loved what I heard, and think I would enjoy being a part of it. I'm attaching my resume. Kindly pass it along to your organization's HR rep? Please open it and let me know if there's anything else you need. Thanks again,

— Jaqueline Canton

[SHOW ME MORE](#)



Even innocent sounding posts can give spear phishers the information they need to craft customized messages. Remember that what you do online is often public, so be sure to minimize the amount of work-related information you share. Click [SHOW ME MORE](#) to see other spear phishing examples.



## Example Spear Phishing Message

 **Sampson, Mark**  
 Wednesday, August 09  
 Anyone know of any good pubs near Paternoster Square?

 **Doug Alderman**  
 You gotta try the Odd Ræt Inn. Run down but the best stouts in the financial district. I think you can get a drink menu and directions [here...](http://motor.geosites.jp/idfqq)

<http://motor.geosites.jp/idfqq>



Even innocent sounding posts can give spear phishers the information they need to craft customized messages. Remember that what you do online is often public, so be sure to minimize the amount of work-related information you share. Click **NEXT** to continue.

# Business Email Fraud

## Definition

---

- **Business Email Fraud/Compromise**
  - When a cyber criminal impersonates a familiar business partner through email.
  - The cyber criminal typically asks for a customer's payment to be redirected to a new account, and, if the ploy works, the recipient of the email instructs the customer to change payment methods, thus paying the cyber criminal instead of the appropriate company.

# Business Email Fraud

## Examples: Mark Sampson

---

- Thursday – Nov 26<sup>th</sup>, 2020

Hello Mark,

You have been selected to participate in the Whitespace pilot for Canada.

Key elements for the opportunities are that Clients are being recommended products that are appropriate for that clients industry.

A note on the data, estimated revenue are only given on certain lines. Lines with blank or 0 revenue are still opportunities there is just no guidance on revenue/premium amounts.

Whitespace – Pilot

<https://app.powerbi.com/groups/0c5230be-821a-43d6-b2a1-60cbe66569e6/reports/86757bc4-a1a3-4658-8ea3-296b9cc3b4c7?ctid=6cacd170-f897-4b19-ac58-46a23307b80a>

If you have never used PowerBI before you will need to set up a free account with your AJG email. It's all single sign on.

Thanks,  
Michael Lewis

# Business Email Fraud

## Examples: Mark Sampson

---

- Friday – Nov 27<sup>th</sup>, 2020

Re: Change of Banking Account:

Afternoon,

We are switching bank account within RBC.

Here are the details. If I need to send anything else please let me know.

Thanks, Claire

# Suggestions on how to combat Business Email Fraud

- **Best Practices:**

- Protect your email system. For cloud-based systems, a key safeguard is to implement a multifactor authentication, which requires more than one step to verify a user's identity.
- Don't trust an email just because the sender's name is familiar. The email account may have been compromised and be under the control of a cyber criminal.
- Never follow new instructions without first verifying with a phone call. Do not reply directly to the email to verify changes – you should always call your business partner to ensure the legitimacy of any changes in the payment process or for other suspicious requests.



# Cyber & Privacy Liability Insurance

## For the Members of PSC





# Cyber & Privacy Liability Insurance

## For the Members of PSC

---

### Covered Claim Scenarios:

- Stolen or lost information
  - stored on paper files, laptops, smartphones or thumb drives.
- Human Error
  - an employee opens an attachment that infects your network with a virus or malware.
- Rogue Employees
  - who have access to sensitive information and intend to harm the organization.
- Computer System Hacked
  - illegal access by a third party causing a disclosure of confidential information or extortion demands.

# Cyber & Privacy Liability Insurance

## For the Members of PSC

---

- Gallagher insures +85% of surveyors across Canada.
- Exclusive Cyber & Privacy Liability Insurance Policy designed for surveyors.
  - We are quoting the coverage for every survey firm we insure during the Professional Liability policy renewal process.
- Dedicated limits, specialized coverage/pricing.
- Policy Territory – anywhere in the “*Universe*”

# Cyber & Privacy Liability Insurance

## For the Members of PSC

---

- **First Party Coverage**
  - Loss to your assets/income
  - Cyber Incident Response:
    - Legal fees, forensics, notification costs, credit monitoring, public relations, etc.
  - Business Interruption:
    - Loss of profits and expenses from interruptions of insured's systems

# Cyber & Privacy Liability Insurance

## For the Members of PSC

---

- **First Party Coverage**
  - Digital Data Recovery:
    - Costs to restore or replace lost or damaged data or software
  - Network Extortion:
    - Payments to prevent digital destruction/impairment

# Cyber & Privacy Liability Insurance

## For the Members of PSC

---

- **Third Party Liability Coverage**
  - Injury to a Third Party
  - Cyber, Privacy and Network Security Liability:
    - Failure to protect private or confidential information of others, and failure to prevent a cyber incident from impacting others' systems
  - Payment Card Loss:
    - Contractual liabilities owed, pursuant to a payment card processing agreement

# Cyber & Privacy Liability Insurance

## For the Members of PSC

---

- Third Party Liability Coverage
  - Regulatory Proceedings:
    - Defence for regulatory actions and coverage for fines and penalties, where insurable by law
  - Media Liability:
    - Copyright and trademark infringement

# Cyber & Privacy Liability Insurance

## For the Members of PSC

---

- **Social Engineering Extension:**
  - \$50,000 - \$150,000 limit
  - Higher limits available



# Cyber & Privacy Liability Insurance

## For the Members of PSC

- Very Competitive Pricing/Limits:

Description	Premium		
	\$500,000	\$1 million	\$2 million
Limit	\$500,000	\$1 million	\$2 million
Revenue <\$10 million	\$965 - \$1,925	\$1,250 - \$2,445	\$1,695 - \$3,650
Revenue >\$10 million	TBA	TBA	TBA
Retention	\$2,500	\$5,000	\$5,000

- *Subject to acceptable answers to underwriting questions*

# Additional Questions?

Please raise your hand...

---

