



29 June 2016

Canadian Council of Insurance Regulators
Secretariat
5160 Yonge St., P.O. Box 85
Toronto, ON, M2N 6L9

ccir-ccrra@fSCO.on.ca

Re: "Electronic Proof of Automobile Insurance Project – Issues Paper"

Introduction

The Canadian Association of Direct Relationship Insurers (CADRI) is a trade association representing insurance companies who offer automobile, home and commercial insurance products to Canadians on a direct basis. Whether through the web, on the phone or face-to-face, CADRI members provide end-to-end service and are in direct relationships with their customers through all steps of the sales and service process.

CADRI monitors the insurance regulatory environment in all provinces and territories and supports regulation that encourages distribution accessibility and efficiency, technological innovation and other measures necessary for a healthy and competitive insurance market for the benefit of all Canadians.

CADRI is pleased to provide comments on the Canadian Council of Insurance Regulators' (CCIR's) May 2016 issues paper on electronic proof of automobile insurance project (EPAI).

CADRI supports steps which would see the acceptance of EPAI as a standard practice across Canada. In the interim, we recommend that provincial jurisdictions move to accept consumer-printed versions of their proof of automobile insurance. We understand that change, and new practices, inevitably raise questions about how to manage the implications of the change. Some of these questions, relative to privacy and the consequences for the law enforcement community, are outlined in CCIR's issues paper. We submit that the implementation of EPAI by some 43 US jurisdictions mitigates many of these concerns.

Benefits of e-proof

Canadians are increasingly comfortable doing a myriad of transactions online and on their smart phones. In fact, customers are now expecting to do more online and with their phones. They are demanding this kind of evolution from service providers such as insurance companies.

According to the Canadian Radio Television and Telecommunications Commission (CRTC), and based on Statistics Canada Household Survey figures, 81.4 percent of Canadians had a wireless phone in 2012¹. Catalyst research shows that 68 percent of Canadians had a smart phone in 2015 – up 24 percent from the previous year.² By 2018, penetration rates for smart phones in demographic bands between 18 and 54 will range from 98 percent to 85 percent.³ Many households, particularly in the 18-to-34-year age bracket use only mobile phones.

¹ <http://www.crtc.gc.ca/eng/publications/reports/PolicyMonitoring/2014/cmr2.htm> Table 2.0.7

² <http://catalyst.ca/2015-canadian-smartphone-market/> Figure 1

³ <http://www.emarketer.com/Article/Over-Half-of-Canadas-Population-Use-Smartphones-2015/1011759>

With this increasingly high penetration of mobile internet access, Canadians are banking, submitting insurance claims, receiving airline boarding passes, and applying for employment through their mobile devices. We would argue that electronic versions of documents have become the norm as most companies move away from paper to offer digital versions available in every type of format and platform (email, pdf, images, on desktop, on website, SMS, on app, etc).

Yet currently, when it comes to proof of auto insurance, consumers take a step back in time. Each year they wait for their new insurance package to arrive in the mail, so that they can pull out their 'pink slip' and place it in a safe location in their vehicles or wallets.

From a consumer perspective there are numerous benefits to being able to print their own proof of auto insurance, or having the option to use EPAI. With an enabling regulatory framework, EPAI would allow customers to email the e-proof certificate among the users of their vehicles, and speed the process of insuring a new vehicle. Currently, when a customer buys a new vehicle, they call their insurance company and receive an email with an updated card which can be printed at home and is valid for 30 days. If this practice works on a temporary basis now, and is acceptable to all the provinces, it could easily become the norm.

It's important to note, the traditional, hard-copy proof of insurance is not a necessity for insurers. When a customer makes a claim, they cite the number of their policy, as opposed to scanning or photographing and sending in a visual of their proof of insurance certificate. The document is largely produced for the law enforcement community.

Precedents for use

The CCIR's May 2016 issues paper on electronic proof of automobile insurance project outlined some stakeholder concerns about the transition to EPAI. The Property Casualty Insurers Association of America (PICCA) reports that 43 US states have enacted legislation which permit some form of EPAI including electronic delivery and use of an electronic image of evidence of coverage.⁴ The US experience provides useful precedents for overcoming concerns about EPAI.

Privacy issues

Privacy is an important issue. People store a lot of personal information on their smart phones. It is a reasonable question to ask whether everyone would be comfortable handing all this information to an enforcement officer in the course of demonstrating that they hold valid automobile insurance. New Jersey, for one, managed this issue by embedding protection for the consumer in its legislation: "The use of a cellular telephone, tablet, computer or any other electronic device to display proof of insurance does not constitute consent for the police officer or judge to access other content on the device."

In addition, numerous US-based insurance companies have developed features on their mobile applications to allow customers to file their e-proof of insurance securely on a device, separate from other information, access and file, view and email it as necessary. These include AllState, Esurance, Geico, Progressive, and State Farm.

If law enforcement questions the validity of EPAI, we recommend that they are not allowed to confiscate the device. In such instances in the US, Michigan authorizes the police officer to require the person to electronically send the digital insurance card to a specified location. In many US jurisdictions, if a driver is unable to provide proof of insurance because their battery has died, law enforcement will give a ticket or a minimal fine. Some state officials issue warnings instead.

There are many other channels to provide proof of insurance, and timelines to produce proof. We recommend that drivers are given a time period to produce proof of insurance in another format whether hard copy or email. In many jurisdictions in Canada, if a driver has left home without their driver's license, they have a period of time to produce it. This approach could be applied to proof of insurance.

Liability

Several US states have laws which release a police officer from liability if a device is damaged during inspection. Michigan's law reads: a police officer "... is not liable for damage to or loss of an electronic device that occurs as a result of a police officer's viewing an electronic copy of a certificate of insurance ... regardless of whether the police officer or the owner or operator of the vehicle was in possession of the electronic device at the time the damage occurred." Similarly, Missouri law releases the police officer, unless they cause the damage intentionally: "...the person presenting such a mobile electronic device shall assume all liability for any damage that may occur to the mobile electronic device, except for damage willfully of maliciously cause by a department employee or agent."

⁴ <http://www.insblogs.com/auto/electronic-proof-still-not-canada/6426>

Other issues

When travelling in the US to jurisdictions where electronic proof is not yet accepted, insurers operating in the US and US regulators recommend that consumers contact their insurer to request a physical insurance card if they plan to travel to a jurisdiction that does not yet permit EPAI. Allowing customers to print their certificate at home would make this easier and more convenient.

On the question of safeguards against fraud, we do not believe that EPAI will create more cases of fraudulent reproduction of proof of insurance. In our estimation, the risk is higher for the printed version – pink or other. If a law enforcement officer has doubts about the validity of the EPAI, they can ask the consumer to produce valid proof of insurance within a reasonable time period.

Moving forward in Canada

CADRI supports CCIR's stance that Canadian insurance regulators have the legal capacity to authorize EPAI delivery and use in their respective jurisdictions. We note that New Brunswick, Nova Scotia and Quebec have taken steps toward drivers using alternative documentation. New Brunswick explicitly allows drivers to present a photocopy of their registration as proof. Nova Scotia leaves room for a photocopy of an insurance card to be used in the case of multiple drivers who use a car on a regular basis. Quebec focuses primarily on the content that is required to demonstrate proof of insurance over the form of the content, and proof of insurance can be emailed.

We recommend that people holding valid auto insurance should be able to receive proof by email from their insurance company or download it via a secure source on their insurance company's website, and print a copy to have available for checks by the law enforcement community. Generally, it is legal in Canada to provide an electronic copy of documentation if the recipient agrees. By agreeing to this measure as an interim step toward EPAI, the CCIR and its members will enable significant change and convenience for auto insurance customers across the country.

CADRI members have discussed the larger project of creating a bar code system for EPAI. We believe such a system would take a long time to launch and could be costly for both insurance companies and law enforcement agencies to implement. It would require that almost every law enforcement vehicle in Canada would need a working bar code scanner. While CADRI does not know how many bar code scanners would be required by enforcement agencies, according to Statistics Canada, there were close to 70,000 police officers in Canada in 2012.⁵ This does give some indication of the extent and volume of any effort to equip police vehicles with scanners. That said, CADRI is open to participating in ongoing dialogue between the concerned parties about the development of a bar code system.

Conclusion

In sum, CADRI supports a move by Canada's auto insurance regulators toward EPAI. We believe there are many benefits of doing so for drivers, insurance companies, and the law enforcement community.

Many of the stakeholder concerns outlined in the CCIR's May 2016 Electronic Proof of Automobile Insurance Project Issues Paper have been considered and overcome in the US.

As an interim measure, CADRI recommends that regulators set in place a framework that allows insurance companies to email, or provide digital access to, proof of insurance to customers who are open to printing their own certificate.

CADRI is confident that a move to EPAI will be a positive one, as few issues have arisen in the 43 US states which have adopted the practice recently.

As CCIR considers this submission and others it received, CADRI would be pleased to consult further with CCIR and discuss these options and others. In addition, CADRI would be pleased to join industry efforts to meet with the law enforcement community to discuss the transition to customer self-printing and EPAI.

Thanks you for the opportunity to provide comment on EPAI.

Yours truly,



Alain Thibault,
President and Chair

⁵ <http://www.statcan.gc.ca/pub/85-225-x/85-225-x2012000-eng.pdf>



Response to the CCIR's Issues Paper on
"Electronic Proof of Auto Insurance"

June 21, 2016



About The Co-operators

The Co-operators is a group of Canadian companies focusing on insurance and financial services. As a co-operative, our 43 member-organizations include co-operatives and credit union centrals representing a combined membership of millions of Canadians.

In Canada, we have over \$35.1 billion in assets under administration, and employ 4,632 individuals and 2,513 licensed insurance representatives, while serving more than 350 credit unions with nearly 5.3 million members.

We insure 722,000 homes, 1 million vehicles, 36,000 farms, and 128,000 businesses.

In 2015, The Co-operators contributed over \$5.8 M to Canadian charities and community organizations across the country.

Stakeholder Concerns

As technology continues to rapidly evolve, we believe it is vital for the insurance industry to meet the demands of clients and stakeholders. As their expectations grow, we must expand with the appropriate tools.

The Co-operators supports the CCIR's recommendation to allow for Electronic Proof of Auto Insurance (EPAI) in Canada, alongside the traditional paper proof of insurance.

In regards to addressing concerns related to operationalizing EPAI, below are recommendations we believe will address **privacy**, **liability** and "**other**" issues as noted in the CCIR's Issues Paper.

Privacy

Will law enforcement be allowed to access other information/ content on electronic devices used to demonstrate proof of insurance?

We recommend insurers investigate technologies that provide privacy blocks to devices when enabled. We hope to see a solution where only the EPAI, and perhaps the app/device wallet that contains this information, could be viewed by law enforcement.

However, we recognize there could be limitations in capabilities of providing this (particularly when considering all electronic device variances).

With any option, we recommend awareness be included in the privacy agreement upon enrolment for EPAI.

If law enforcement questions the validity of EPAI, are they allowed to confiscate the electronic device?

In cases where an officer lays a charge for fraud, the officer should have the ability to confiscate a device for use as evidence. Otherwise, we do not support law enforcement confiscating the electronic device.

Liability

Who is responsible if electronic devices used to demonstrate proof of insurance, such as mobile devices are damaged during inspection?

If a third party negligently or wilfully damages a device while it is in their possession, they should be liable for that damage. Otherwise, the insured/device owner should assume liability for their own device. Affirmative confirmation of the assumption of this risk should be included in the enrolment wording agreement for EPAI. Many device owners already assume this risk today at retail locations, movie theatres, etc. We hope this to be a minimal risk for the most part.

“Other”

What is considered ‘reasonable inspection’ for law enforcement handling electronic devices?

We recommend following the processes currently in place today with paper liability slips. If the Police Officer feels they need to take the device back to their vehicle along with the driver’s license and vehicle ownership, it should be considered reasonable to do so.

We strongly believe that any third party, including the police, should not have access to anything else on the device without a warrant, and that handing over a device with an insurance card visible should not be taken as consent that the third party can access anything on the device.

It would be prudent to advise our clients of the potential for third parties to accidentally or intentionally view other things on their phone, and have them affirmatively confirm that they are aware of this potential prior to providing them with electronic proof of insurance.

When traveling to a jurisdiction that does not yet allow for the EPAI, what steps must be taken?

We believe having the option for clients to print-on-demand from their device will address these types of circumstances. The recommended solution being, they could print the paper

copy from home before travelling to other jurisdictions that do not support EPAI and be prepared for these situations.

If an electronic device malfunctions, has no network access or is out of power, how will law enforcement handle such issues?

As discussed, if provided the option for clients to print-on-demand from their own device, insureds would have a paper-copy as back-up to provide to law enforcement in these given situations.

In the case of no network access, EPAI solutions could be developed to be stored in the electronic device in a way that was viewable with no network access availability. Once initially downloaded to device, the electronic proof could be viewed without the requirement of network access.

In regards to device out of power, as a whole, most people are cautious of their device charge as we heavily rely on our devices for several day to day needs in today's society. Furthermore, this also could be included in part of the awareness/ warnings in terms of agreement when electronic proof is requested by clients.

We recommend following the same processes that are in place today for validating paper insurance; which is law enforcement providing insureds 24 hours to produce proof of insurance. We believe the onus of providing valid proof of insurance rests with the client as long as all reasonable solutions have been given and promoted by the Insurers.

As long as the onus continues to be on the insured to provide valid proof of insurance, and that the insurance company has provided the client with a paper copy, PDF, or an in app card (as mandated by the relevant regulator) the insurer should bear no responsibility, just like today, for an insured's inability to provide proof of insurance.

If the owner of a vehicle gives permission to third party to use their vehicle, how does electronic proof of insurance work in such cases?

Having the option for clients to print their liability slip would greatly reduce this risk. The insured could choose to leave the printed paper liability slip in their vehicle or provide to the third party while loaning their vehicle.

Moreover, an option within the app/wallet should be considered to allow forwarding the proof to an alternate email. The EPAI should be a protected document that does not enable editing capabilities.

While photocopies of proof of insurance are not permissible, will insureds be allowed to print paper copies of proof of insurance cards emailed to them by their insurer?

We recommend the client has the option to print-on-demand in black and white on plain paper (and re-print as needed) as part of their device capability options; rather than the need for Insurers having to send. This is our recommendation to eliminate/reduce many of the potential concerns addressed.

Furthermore for the industry to benefit from this convenience from a cost-savings perspective, we do not feel that insurance companies should be required to mail and/or email liability slips in addition to the clients that choose the option to receive their liability slips electronically.

Another option would be an electronic service portal that a client could access via password and print-on-demand.

Most significantly, our clients would benefit from the ease of being able to print from home/work, and re-print if misplaced or needed for an additional party – without having to contact their insurance representative only for this reason.

Will electronic proof of insurance apply to all classes of vehicles?

Yes, we recommend having this option provided to all classes of vehicles. We see this benefiting and providing convenience to all vehicle classes.

What kind of safeguards should be in place to prevent the fraudulent use of electronic proof of insurance?

We believe there should be document protection in place (not able to edit).

Supplementary Initiatives

The use of barcodes as a supplementary innovative initiative has been raised for consideration by the Electronic Commerce Committee (ECC). It recognizes it as a longer term consideration as it would require a great amount of time, coordination, and adoption upfront by insurers and law enforcement.

We believe that all stakeholders must be considered with Insurers solutions. For example, law enforcement and provincial ministries must have the capabilities and be equipped to work with our technology based solutions.

Concluding Remarks

The technology environment, as well as insurers, are moving at a fast rate to adopt and advance the ability to service clients in a digital expectations age, while providing ongoing enhanced services to assist them in their daily needs, or at times of urgency.

This is being done while also adopting policy changes that foster other environmental considerations that benefit our communities and customers through such measures as Sustainability initiatives and overall paperless services for our customers.

Recognizing the speed of technological change within the marketplace, we recommend focus be placed on ensuring both flexibility and ease of decision making for possible integrated enhancements measures governing this area.

This flexibility should allow insurers to easily embrace consumer experience servicing enhancements (integrating them with EPAI capabilities) within the spirit that all mandatory requirements are met regarding delivery and privacy stipulations set out.



Thank you once again for the opportunity to provide comments on the Issues Paper. If you have any further questions, or require clarification, please do not hesitate to contact me directly at maya_milardovic@cooperators.ca.

With best regards,

A handwritten signature in cursive script that reads "Maya Milardovic".

Maya Milardovic
Director, Government Relations
The Co-operators Group Limited

June 24, 2016

Patrick Déry
Chair, Canadian Council of Insurance Regulators
Place de la Cité, tour Cominar
2640, boulevard Laurier, bureau 400
Québec (Québec) G1V 5C1

Dear Mr. Déry,

We have reviewed the CCIR's Electronic Commerce Committee (ECC) *Electronic Proof of Automobile Insurance Project* issues paper and are excited to see this initiative move forward. Establishing a framework for permitting electronic proof of automobile insurance (EPAI) will support the insurance industry in meeting the needs of today's tech-savvy consumer. We would like to take this opportunity to submit our proposal for CSIO's role in driving this initiative, as well as share our thoughts and recommendations regarding some of the concerns tabled in the issues paper.

Proposal: Development of Standards and Protocol for EPAI

CSIO is a national association with over 35 years of serving the insurance industry by translating insurance data and regulations into authoritative standards and forms, supporting the secure and efficient exchange of electronic policy data between trading partners. In fulfilling this mandate, we work closely with industry stakeholders and provincial regulators to ensure that resources such as CSIO's provincial auto insurance applications accurately reflect evolving requirements.

CSIO data standards have evolved to include the secure and robust eDocs standard, which the industry uses to send full PDF policy documents – over 20,620,000 in 2015 alone. eDocs also serve as the foundation of our eDelivery solution, which leverages Canada Post's secure epost platform to deliver policy documents directly to consumers' digital mailboxes.

We propose that CSIO leverage its expertise to:

- develop the standards and protocols for the creation of uniform, authoritative EPAI, including a provision that the display of EPAI on electronic devices complies with privacy requirements
- establish the visual design of EPAI for display in electronic and printed form, including both policy information and standardized Certificate conditions and warning verbiage

In this proposal, third parties such as insurers and brokers would implement these standards to develop their own proprietary mobile applications for consumers to obtain, store and display their EPAI. To insure the standards remain up to date, CSIO would hold working groups with industry stakeholders to review and update the requirements for EPAI on a regular basis, making updates as needed.

CSIO is also prepared to develop a single, authoritative mobile application for consumer use in place of multiple, proprietary applications, should industry consensus indicate a preference for such a solution. In this way, CSIO would fulfill the same role for EPAI as Informco does for pink slips: a trusted and centralized provider of insurance documentation for the insurance industry.

Stakeholder Concerns

We recognize that there is a gap between the regulations and policies that are currently in place and those that are required to support EPAI. After carefully reviewing the stakeholder concerns identified in the ECC issues paper, we feel that the gap is minimal, and easily bridged. In fact, there are many direct correlations between the current procedures for pink slips and what would be required for EPAI, indicating the strong likelihood of a simplified and streamlined transition for all jurisdictions across Canada.

	Stakeholder Concern	Resolution
Privacy	Will law enforcement be allowed to access other information/content on electronic devices used to demonstrate proof of insurance?	<ul style="list-style-type: none"> - direct correlation with current restrictions on law enforcement regarding unlawful search - Scope of access to electronic devices by police to be determined by regulation, as seen in American law (Appendix A) - App may automatically lock screen of device when displaying EPAI
	If law enforcement questions the validity of EPAI, are they allowed to confiscate the electronic device?	<ul style="list-style-type: none"> - direct correlation with current law enforcement practice to validate coverage by calling insurer directly (Appendix B)
Liability	Who is responsible if electronic devices used to demonstrate proof of insurance, such as mobile devices, are damaged during inspection?	<ul style="list-style-type: none"> - Liability to be determined by regulation, as seen in American jurisdictions (see Appendix A)
Other	What is considered “reasonable inspection” for law enforcement handling of electronic devices?	<ul style="list-style-type: none"> - Extent of reasonable inspection to be determined by regulation, as seen in American law (Appendix A)
	When traveling to a jurisdiction that does not allow for EPAI, what steps must be taken?	<ul style="list-style-type: none"> - direct correlation with current practice, where onus is on individuals to know and obey local laws (<i>e.g.</i>, right-hand turns on red lights are permissible in Quebec, but not the Island of Montreal) - CCIR to implement one uniform regulation for EPAI across Canada

	Stakeholder Concern	Resolution
	If an electronic device malfunctions, has no network access or is out of power, how will law enforcement handle such issues?	<ul style="list-style-type: none"> - direct correlation with current practice, which permits law enforcement to issue a ticket or allow a specified period of time for driver to present proof of insurance - Requirement for mobile app to store offline EPAI on devices
	If the owner of a vehicle gives permission to third party to use their vehicle, how does electronic proof of insurance work in such cases?	<ul style="list-style-type: none"> - Standards could enable vehicle owners to grant temporary permission to third party to download, store and display EPAI - Owner could provide printed copy in lieu of EPAI
	While photocopies of proof of insurance are not permissible, will insureds be allowed to print paper copies of proof of insurance cards emailed to them by their insurer?	<ul style="list-style-type: none"> - Regulations should be updated to allow plain white paper in place of pink paper, specifying a standardized design for proof of insurance whether printed or electronic - Owners may still request that insurer send a paper copy
	Will electronic proof of insurance apply to all classes of vehicles?	<ul style="list-style-type: none"> - direct correlation with current practice, where pink card applies to all classes of vehicles
	What kind of safeguards should be in place to prevent the fraudulent use of electronic proof of insurance?	<ul style="list-style-type: none"> - Standards could include encryption for creation, transmission and storage of EPAI - Existing features of drivers' mobile devices (encryption, passcode, biometrics, etc.) provide security for display of EPAI - Security requirements to be identified and addressed through stakeholder consultations

EPAI is a natural extension of CSIO's work, building on our track record of developing secure, authoritative and compliant data standards and solutions for use within the insurance industry. We would be pleased to work with CCIR and the ECC to establish the standards, protocols, and perhaps even the end-user application for EPAI that meets the requirements identified in collaboration with industry stakeholders.

If you have any questions, please do not hesitate to contact me.

Sincerely,



Catherine Smola
President & CEO

Phone: 416-360-1773 ext. 2327

Email: csmola@csio.com

cc:

Hélène Samson

Chair, Electronic Commerce Committee

Appendix A - Ohio Revised Code

The underlined provisions reflect the amendments to the Ohio Revised Code¹:

Sec. 4509.101. (G)(1)(a) The registrar, court, traffic violations bureau, or peace officer may require proof of financial responsibility to be demonstrated by use of a standard form prescribed by the registrar. If the use of a standard form is not required, a person may demonstrate proof of financial responsibility under this section by presenting to the traffic violations bureau, court, registrar, or peace officer any of the following documents or a copy of the documents:

(i) A financial responsibility identification card as provided in section 4509.103 of the Revised Code;

(b) A person also may present proof of financial responsibility under this section to the traffic violations bureau, court, registrar, or peace officer through use of an electronic wireless communications device as specified under section 4509.103 of the Revised Code.

[...]

(N)(1) When a person utilizes an electronic wireless communications device to present proof of financial responsibility, only the evidence of financial responsibility displayed on the device shall be viewed by the registrar, peace officer, employee or official of the traffic violations bureau, or the court. No other content of the device shall be viewed for purposes of obtaining proof of financial responsibility.

(2) When a person provides an electronic wireless communications device to the registrar, a peace officer, an employee or official of a traffic violations bureau, or the court, the person assumes the risk of any resulting damage to the device unless the registrar, peace officer, employee, or official, or court personnel purposely, knowingly, or recklessly commits an action that results in damage to the device.

Sec. 4509.103. (A) As used in this section and sections 4509.101 and 4509.102 of the Revised Code, "electronic wireless communications device" includes any of the following:

(1) A wireless telephone, including a cellular telephone;

(2) A personal digital assistant;

(3) A computer, including a laptop computer, a netbook computer, and a tablet computer;

(4) Any other substantially similar wireless device that is designed or used to communicate and displays text or images.

¹ U.S., H.F. 307, *An Act relating to transportation; commerce; providing for proof of insurance in electronic format; amending Minnesota Statutes 2014, section 169.791, subdivision 1, 2,* 89th Leg., Reg. Sess., Minn., 2015 (enacted).

Appendix B – Excerpt from CSIO *eSlips Advisory Report*

3. Issue of Fraud

Over the past 10 years, modernization of the pink card regime has been proposed from time to time in the course of various reviews of automobile insurance regimes. In Ontario, the Superintendent's 2009 Report on the Five Year Review of Automobile Insurance to the Minister of Finance², the Superintendent indicated that the "primary concern regarding electronic commerce is the production of fraudulent liability cards". The report also noted that "fraudulent paper liability cards currently exist and that technological solutions may exist to address these concerns."

However, citing fraud as a basis to rely on a paper card, seems incongruous with current technology. Specifically:

- Technological solutions exist which can securely deliver authentic insurance cards by electronic means.
- Bad actors can create or use a false insurance card regardless of whether the insurance card is in paper or electronic form, and without any appreciable difference in difficulty as between a paper or electronic form.
- It is relatively easy for bad actors to make use of an invalid insurance card (*e.g.*, one for which the underlying insurance has been cancelled) regardless of its form. Police officers inevitably accept paper insurance cards that appear valid and unexpired.
- There is no technological solution that police officers can use in the field to verify current proof of insurance coverage. At best, officers may be able to access provincial databases that indicate whether the vehicle was insured at the time of vehicle registration or renewal. This stale information is not particularly helpful in detecting fraudulent paper liability cards.
- **All police agencies consulted in connection with this advisory report³ suggested that if an officer doubted proof of valid insurance, a call to the insurance company would be the easiest way to verify the claim (an approach that seems to be taken regardless of whether the insurance is Canadian or U.S.).** [emphasis added]

Given this, it is difficult to see how fraud prevention can continue to justify the original paper card requirement to the exclusion of an electronic card.

² <https://www.fsco.gov.on.ca/en/auto/5yr-review/Documents/FiveYearReviewReport.pdf> [March 31, 2009].

³ The Royal Canadian Mounted Police, the Ontario Provincial Police, the Toronto City Police, and the Calgary Police.

June 29, 2016

Canadian Council of Insurance Regulators (CCIR) Secretariat
5160 Yonge Street, Box 85
Toronto, Ontario M2N 6L9

Delivered by email to: ccir-ccrra@fSCO.gov.on.ca

Dear Members of the Electronic Commerce Committee,

Re: Electronic Proof of Automobile Insurance Project Issues Paper

On behalf of Desjardins General Insurance Group (DGIG), I am writing to comment on the Canadian Council of Insurance Regulator's (CCIR) Electronic Proof of Automobile Insurance (EPAI) Project Issues Paper.

DGIG is a subsidiary of Desjardins Group, the leading cooperative group in Canada with over \$229 billion in total assets. With over 4 million policies in force, DGIG is one of the top three P&C insurers in Canada.

DGIG strongly supports the CCIR's recommendation to its constituent regulators to make EPAI a reality across Canada.

We have also reviewed the submissions from the Insurance Bureau of Canada (IBC) and the Canadian Association of Direct Relationship Insurers (CADRI) and are in agreement with the comments provided.

Many of the concerns cited in the CCIR paper have been considered and overcome in the United States. While helpful to resolve, it's important to note that they are not prerequisites to introducing EPAI.

We encourage the CCIR and its constituent regulators to build on its momentum and introduce benefits to consumers as soon as possible. For example, CCIR can immediately recommend that consumers holding valid auto insurance be able to receive proof by email from their insurance company, or download it via a secure source on their insurer's website, and print a copy to provide as needed to law enforcement. This change would not require legislation, would provide convenience for consumers and would not negatively impact law enforcement. Our industry could implement this consumer benefit quickly.

Ultimately, after some further consultation on the concerns raised by stakeholders, it is important to move quickly towards EPAI on smartphones. We look forward to participating in those upcoming stakeholder consultations.

We believe that allowing EPAI would benefit consumers, governments, law enforcement and insurers. As discussed in the Paper, a partial structure already exists. The authority for the use of EPAI lies with insurance regulators in most jurisdictions and Canadian electronic commerce laws are already in place. Canada can benefit from existing solutions in the United States to address the remaining issues.

Thank you for the opportunity to provide our commentary. We would be pleased to consult further with CCIR and discuss these options and others.

Sincerely,



Denis Dubois
Desjardins General Insurance Group

Digital pink cards: One giant leap in the right direction

The dawn of the digital age is upon us. We can deny it, we can pretend it's not happening, but the fact of the matter is, we need to adapt to the changing demands of our clients. As more and more companies develop innovative digital solutions for their modern consumers, the more pressure we feel as an industry to keep up with these shifting expectations. All we need to do is look at the financial industry, which has been the driving force of ingenuity over the past decade, to see how much the service industry has changed. From mobile banking to digital wallets, including Apple pay, there is no limit to what we can do from our phones. Yet why do we, as an industry, resist the idea of carrying and accepting digital insurance proof? As the communications manager for Sharp Insurance, people ask me all the time: "Do your clients even care about a mobile app for insurance?" The answer is yes. We have over 6000 clients signed up on our app, and 60% of them use the app for accessing their pink card! Now that we know Canadians are interested, let's examine some of the concerns outlined by the issues paper released by the CCIR, and viable solutions that could transform a very good idea into a reality.

CCIR Concerns, Sharp Answers:

- 1) Will law enforcement be allowed to access other information/content on electronic devices used to demonstrate proof of insurance?

Our recommendation for this issue is to restrict the information law enforcement can access to the pink card itself. There is no need for law enforcement to access information other than proof of insurance. This is a violation of privacy.

- 2) If law enforcement questions the validity of EPAI, are they allowed to confiscate the electronic device?

As digital pink cards are a second option for providing proof of insurance, it is therefore not necessary for the officer to confiscate the mobile device. A quick call to the insurance provider to confirm its validity should be more than sufficient. It should also be the responsibility of law enforcement to know what constitutes valid digital proof.

- 3) When travelling to a jurisdiction that does not yet allow for the EPAI, what steps must be taken?

The responsibility should be with the insured to know the rules concerning digital pink cards in the territory they reside in, or travelling to.

- 4) If an electronic device malfunctions, has no network access, or is out of power, how will law enforcement handle such issues?

Law enforcement should handle the issue the same way they would if the client had expired pink cards or no pink cards in the vehicle. Give the insured a ticket, and then the insured can dispute the ticket after the fact. On the technology end, we could program the mobile app to keep a cached copy of the pink card, that way, it is accessible even when there is not internet connection.

- 5) If the owner on a vehicle gives permission to third party to use their vehicle, how does electronic proof insurance work in such cases?

The insured should be allowed to email a digital copy of the pink card to any individuals borrowing the vehicle. In the USA, where 43 States accept digital pink cards, digital PDFs of pink cards are legal, and widely used.

- 6) What kinds of safeguards should be in place to prevent the fraudulent use of electronic proof of insurance?

If we use the USA as an example, many of the states stipulate that proof of digital insurance should be as follows: From a trusted insurer mobile application, or a digital PDF. Pictures of a pink card are not accepted. By signing into an insurer or broker app in front of law enforcement will significantly reduce the risk of fraudulent activity. After all, designing, coding, and producing a mobile app is a lot of work, and it's doubtful that people would go so far to do that in order to avoid insurance payments. Even so, fraud exists in many places, and therefore we would need to proceed with some level of caution, as we do now, with paper proof of insurance.

These are a few of our recommendations. Digital proof of insurance is a step in the right direction. Change is inevitable: whether it's today or in a few years from now, digital pink cards will become the accepted norm, so let's put the province of Alberta and the rest of Canada on the map for being progressive and innovative by being early adaptors of digital proof.

June 30, 2016

CCIR Secretariat
5160 Yonge Street, Box 85
Toronto, Ontario M2N 6L9

ccir-ccra@fscs.gov.on.ca

IBAO Response to CCIR's Electronic Proof of Automobile Insurance (EPAI) Issues Paper

Thank you for the opportunity to comment on CCIR's Electronic Proof of Automobile Insurance (EPAI) Issues Paper.

The Insurance Brokers Association of Ontario (IBAO) represents 12,000 insurance brokers who service six million policyholders in the Province of Ontario. Insurance brokers are highly-trained professionals with very strong community ties. Their priority is to serve the best interest of the consumer, from the initial product selection through client advocacy with insurers in the event a claim is made. Insurance brokers are also business people, mainly small and medium-sized businesses.

Headquartered in Toronto, IBAO Staff oversees the development and implementation of education, policy and administrative matters as directed by the IBAO Board of Directors. The IBAO Board is comprised of 13 elected Directors and 5 elected Executive members from cities and towns throughout the Province of Ontario.

Over the years, IBAO has been an important voice within the insurance industry and to government regarding a number of policy-related issues that affect consumers and brokers, whose interests are intertwined: both require a transparent market in order to function optimally; one that is accessible, accountable, efficient, and fair.

IBAO strongly supports implementation of Electronic Proof of Automobile Insurance (EPAI). We would like to see it implemented as soon as possible.

The CCIR paper posed a number of questions. IBAO is only responding to those questions we believe lie within our area of expertise. The following is our response:

If an electronic device malfunctions, has no network access or is out of power, how will law enforcement handle such issues?

The driver/owner should have 24 hours to bring in a working phone or paper slip.

If the owner of a vehicle gives permission to a third party to use their vehicle, how does electronic proof of insurance work in such cases?

A paper copy should still be available and sent to the insured on renewal. Consumer notification needs to be made that the paper copy or an electronic copy is still valid and should be in the vehicle or with the permitted driver. If it isn't, they should have 24 hours to bring in a working phone or paper slip.

While photocopies of proof of insurance are not permissible, will insureds be allowed to print paper copies of proof of insurance cards emailed to them by their insurer?

No. Paper copies should still be sent out with the renewal documents, and additional copies could be requested from broker, agent or company. There will be a segment of people who will move to the paperless procedure; therefore, both methods need to be in place.

Will electronic proof of insurance apply to all classes of vehicles?

IBAO believes that EPAI should only be available for commercially rated vehicles owned and operated by the owner or their family member and private passenger vehicles. Due to the complications in administering electronic liability slips for a Fleet policy or a Garage Auto Policy, we do not believe this should be implemented at this stage, if at all.

What kind of safeguards should be in place to prevent the fraudulent use of electronic proof of insurance?

The police should still be able to log into the Ministry database to ensure that the vehicle is insured at the site of an accident or police pull over. This occurs currently, and there is no reason for this double check to be stopped. There would need to be some type of documentation on the electronic slip, as there is now on paper copies e.g. watermark or digital encryption, to ensure that it is valid.

Should you have any questions, please do not hesitate to contact the undersigned.

Regards,



Colin M Simpson
Interim Chief Executive Officer
Cell: 416.407.0677
csimpson@ibao.on.ca

June 30, 2016

RECEIVED
July 5/16

CCIR Secretariat
5160 Yonge Street, Box 85
Toronto, Ontario M2N 6L9

ccir-ccra@fscsco.gov.on.ca

IBAO Response to CCIR's Electronic Proof of Automobile Insurance (EPAI) Issues Paper

Thank you for the opportunity to comment on CCIR's Electronic Proof of Automobile Insurance (EPAI) Issues Paper.

The Insurance Brokers Association of Ontario (IBAO) represents 12,000 insurance brokers who service six million policyholders in the Province of Ontario. Insurance brokers are highly-trained professionals with very strong community ties. Their priority is to serve the best interest of the consumer, from the initial product selection through client advocacy with insurers in the event a claim is made. Insurance brokers are also business people, mainly small and medium-sized businesses.

Headquartered in Toronto, IBAO Staff oversees the development and implementation of education, policy and administrative matters as directed by the IBAO Board of Directors. The IBAO Board is comprised of 13 elected Directors and 5 elected Executive members from cities and towns throughout the Province of Ontario.

Over the years, IBAO has been an important voice within the insurance industry and to government regarding a number of policy-related issues that affect consumers and brokers, whose interests are intertwined: both require a transparent market in order to function optimally; one that is accessible, accountable, efficient, and fair.

IBAO strongly supports implementation of Electronic Proof of Automobile Insurance (EPAI). We would like to see it implemented as soon as possible.

The CCIR paper posed a number of questions. IBAO is only responding to those questions we believe lie within our area of expertise. The following is our response:

If an electronic device malfunctions, has no network access or is out of power, how will law enforcement handle such issues?

The driver/owner should have 24 hours to bring in a working phone or paper slip.

If the owner of a vehicle gives permission to a third party to use their vehicle, how does electronic proof of insurance work in such cases?

A paper copy should still be available and sent to the insured on renewal. Consumer notification needs to be made that the paper copy or an electronic copy is still valid and should be in the vehicle or with the permitted driver. If it isn't, they should have 24 hours to bring in a working phone or paper slip.

While photocopies of proof of insurance are not permissible, will insureds be allowed to print paper copies of proof of insurance cards emailed to them by their insurer?

No. Paper copies should still be sent out with the renewal documents, and additional copies could be requested from broker, agent or company. There will be a segment of people who will move to the paperless procedure; therefore, both methods need to be in place.

Will electronic proof of insurance apply to all classes of vehicles?

IBAO believes that EPAI should only be available for commercially rated vehicles owned and operated by the owner or their family member and private passenger vehicles. Due to the complications in administering electronic liability slips for a Fleet policy or a Garage Auto Policy, we do not believe this should be implemented at this stage, if at all.

What kind of safeguards should be in place to prevent the fraudulent use of electronic proof of insurance?

The police should still be able to log into the Ministry database to ensure that the vehicle is insured at the site of an accident or police pull over. This occurs currently, and there is no reason for this double check to be stopped. There would need to be some type of documentation on the electronic slip, as there is now on paper copies e.g. watermark or digital encryption, to ensure that it is valid.

Should you have any questions, please do not hesitate to contact the undersigned.

Regards,



Colin M Simpson
Interim Chief Executive Officer
Cell: 416.407.0677
csimpson@ibao.on.ca

Response to CCIR's Issues Paper

Electronic Proof of Automobile Insurance Project

~ June 2016 ~



Introduction

Insurance Bureau of Canada (IBC) supports the Canadian Council of Insurance Regulators' (CCIR) efforts towards allowing more opportunities for consumers to interact with their insurers using electronic means. Electronic proof of automobile insurance (EPAI) would be a more convenient option for many consumers than having to carry the traditional paper copy.

Regulators in Canada already have the authority to permit EPAI. The concerns that CCIR describes in the issues paper are valid. Many of them will require legislation. But, the legislative process should not hold up the introduction of EPAI in the market.

The state governments from more than forty U.S. jurisdictions have approved the use of EPAI. Many of them, but not all of them, passed legislation to address the concerns that CCIR identified. For instance, Idaho, which in 2012, became the first state to permit EPAI, did not have any accompanying legislation. Idaho's experience and the experience in several other states show that legislation to address the concerns in CCIR's issues paper is not a prerequisite for permitting EPAI.

The following sections contain IBC's views and advice pertaining to the concerns that CCIR identified and the supplementary initiatives described in the issues paper.

CCIR Concerns

Will law enforcement be allowed to access other information/content on electronic devices used to demonstrate proof of insurance?

Several U.S. jurisdictions addressed this concern by prescribing in legislation that law enforcement can view only the EPAI document on the device. Below is an example of a legislative provision in New Jersey.

“The use of a cellular telephone, tablet, computer, or any other electronic device to display proof of insurance does not constitute consent for a police officer or judge to access any other content on the device.”

If law enforcement questions the validity of EPAI, is it allowed to confiscate the electronic device?

There is no U.S. jurisdiction that IBC examined that expressly permits law enforcement to confiscate an individual's electronic device if it doubts the authenticity of the EPAI document. However, certain states have addressed this concern to a degree. Below is an example of a legislative provision in Michigan.

“A police officer may require the person to electronically forward the electronic copy of the certificate of insurance to a specified location provided by the police officer. The police officer may then view the electronic copy of the certificate of insurance in a setting in which it is safe for the officer to verify that the



information contained in the electronic copy of the certificate of insurance is valid and accurate.”

This provision permits law enforcement to attempt to verify the authenticity of the EPAI without the risk of damaging the electronic device or accidentally viewing private personal information that is stored on the device.

Who is responsible if electronic devices used to demonstrate proof of insurance, such as a mobile device, are damaged during inspection?

Several U.S. jurisdictions addressed this concern by prescribing in legislation that the operator of the vehicle is responsible for any and all damage to his/her electronic device if he/she uses it to show proof of insurance. However, some states have added provisions to their legislation to protect consumers from a law enforcement officer intentionally causing damage to the electronic device. Below is an example of a legislative provision in Missouri that has this added consumer protection measure.

“...the person presenting such mobile electronic device shall assume all liability for any damage that may occur to the mobile electronic device, except for damage willfully or maliciously caused by a department employee or agent.”

What is considered “reasonable inspection” for law enforcement handling electronic devices?

There is no U.S. jurisdiction that IBC examined that defined “reasonable inspection” in its legislation. However, some states have provisions in their legislation that are meant to limit the amount of time that a law enforcement officer can handle an electronic device. Below is an example of a legislative provision in New York that uses the word “temporarily” to indicate the amount of time that a law enforcement officer is expected to handle an electronic device.

“A driver may temporarily surrender his or her personal electronic device to law enforcement personnel for the purpose of providing proof of insurance through an electronic insurance ID card.”

When traveling to a jurisdiction that does not yet allow for the EPAI, what steps must be taken?

This situation is quite common. Law enforcement in several states and provinces is already dealing with vehicle owners having different forms of proof of auto insurance. For instance, in the Pacific Northwest and the Prairies:

- Vehicle owners in British Columbia have a traditional card or a decal on the vehicle’s license plate;
- Vehicle owners in Alberta have the traditional financial responsibility card; and
- Vehicle owners in Idaho, Montana and Washington have EPAI or a paper copy.



If an electronic device malfunctions, has no network access or is out of power, how will law enforcement handle such issues?

Most U.S. jurisdictions permit an EPAI document to be downloaded to an electronic device. This way, a driver can provide the document to a law enforcement officer even if he/she does not have network access. Since EPAI is voluntary, it is the responsibility of the driver to ensure that his/her electronic device has adequate battery life. Otherwise, he/she may be fined. This is similar to the current situation whereby a driver must ensure that he/she has a proof of insurance card with him/her in case it is requested by a law enforcement officer.

If the owner on a vehicle gives permission to a third party to use his/her vehicle, how does electronic proof of insurance work in such cases?

Many U.S. jurisdictions consider a digital photograph of the original proof of insurance card to be valid. Accordingly, a vehicle owner could electronically send the EPAI document to an individual who is borrowing his/her vehicle. The apps of several insurers in the United States, such as GEICO, Liberty Mutual and Progressive, allow policyholders to download their EPAI document, which can then be electronically sent to another individual.

While photocopies of proof of insurance are not permissible, will insureds be allowed to print paper copies of proof of insurance cards emailed to them by their insurer?

There is no U.S. jurisdiction that IBC examined that addressed this concern explicitly. However, in practice, it seems that printed copies of proof of insurance are valid. For instance, GEICO's app allows policyholders to print the EPAI document.

Will electronic proof of insurance apply to all classes of vehicles?

In every U.S. jurisdiction that permits EPAI, the classes of vehicles that traditionally have been required to have a paper version of the proof of insurance are the ones that now can have EPAI. Below is an example of a legislative provision in Idaho that is common throughout the United States.

*A certificate or proof of liability insurance shall be in the possession of the operator of every motor vehicle or present in every motor vehicle at all times when the vehicle is operated within this state. The certificate or proof of liability insurance shall be provided for inspection to any peace officer upon request to the operator of any motor vehicle... **The certificate or proof of liability insurance required by this section may be produced in either paper or electronic format. Acceptable electronic formats include display of electronic images on a cellular phone or any other type of portable electronic device.***



What kind of safeguards should be in place to prevent the fraudulent use of electronic proof of insurance?

Overall, EPAI will help reduce fraud. Many insurers operating in the United States have developed sophisticated apps that allow a driver to retrieve his/her proof of insurance upon request. The app will only display the proof of insurance if the individual is insured at that given time. With the current paper-based proof of insurance, an individual can purchase insurance, receive the proof of insurance in the mail and then cancel the policy while still retaining a document that shows proof of insurance.

Supplementary Initiative – Centralized Automobile Insurance Database

A barcode on an EPAI document and a centralized automobile insurance database like the Insurance Validation Program (IVP) in Ontario will reduce the number of instances when law enforcement has to take possession of a driver's electronic device for the purpose of viewing the EPAI document. But, implementing initiatives of this nature will be a massive undertaking. They should not be a prerequisite for permitting EPAI in the market.

Also, these types of initiatives will require certain exemptions to accommodate types of policies that do not assign proof of insurance documents to specific vehicles, such as fleet and garage policies.

Conclusion

Permitting EPAI will provide many benefits to consumers, governments, law enforcement and insurers. The provincial insurance laws already authorize the regulators to permit the use of EPAI and develop parameters for its use, like they have done for the paper-based proof of insurance cards.

The laws that have been passed in over forty U.S. jurisdictions provide a template for addressing the concerns described in CCIR's issues paper. Nevertheless, the experience in the United States shows that addressing these concerns is not a prerequisite for permitting EPAI. Accordingly, IBC recommends that the regulators begin a process for allowing insurers to bring EPAI to the market.



June 30, 2016

CCIR Secretariat
5160 Yonge Street, Box 85
Toronto, Ontario M2N 6L9
Via email: ccir-ccra@fsc.gov.on.ca

Re: CCIR's Electronic Proof of Automobile Insurance Project Issues Paper

Members of the CCIR Electronic Commerce Committee,

TD Insurance is pleased to provide a response to the Electronic Proof of Automobile Insurance Project Issues Paper from the Canadian Council of Insurance Regulator's Electronic Commerce Committee.

Established in 1949 TDI is a member of TD Bank Group. TDI is the largest direct response insurer and fourth largest auto and home insurer in Canada, with more than 2.14 million policies and more than \$3.1 billion in written premiums as of April 2016. Through our credit protection products, TDI is also the number one distributor of critical illness insurance. TDI employs more than 3,900 people across Canada, with offices in Ontario, Alberta, Québec, Nova Scotia and New Brunswick. We are committed to working with the government to create a healthy regulatory environment that is efficient, affordable, cost effective and sustainable while meeting the insurance needs of Canadian consumers.

As an insurer providing auto coverage to a diverse population across the country, TD Insurance is always looking for ways to better serve consumers, most often through our own innovations and at times in response to consumer demand. Requests for electronic documentation in general and specifically electronic proof of auto insurance are increasing in number. These requests don't come as a surprise given the shift to electronic documentation and transactions across a variety of sectors: airlines accept electronic tickets and boarding passes, event venues and movie theatres are increasingly using electronic ticketing, hundreds of loyalty programs provide digital cards to their members, and most recently major Canadian banks are allowing customers to use their credit and debit cards with digital wallets. The insurance industry is lagging far behind, and TD Insurance appreciates the regulators' work in this area and looks forward to working with the CCIR, law enforcement and the industry to implement this essential innovation.

In the meantime, an easily made change could offer increased convenience and improved service to insurance customers across the country: consistency in the rules respecting photocopies of proof of insurance, or proof printed at home. New Brunswick allows drivers to present a photocopy of their vehicle registration, but there's no mention in the legislation of proof of insurance. Legislation in Nova

Scotia leaves room for a photocopy of an insurance card to be used where multiple drivers use a single vehicle on a regular basis. Legislation in Quebec focuses on the information required to demonstrate proof of insurance rather than what form that proof takes, and insurers can provide temporary proof of insurance to their customers by email allowing them to print and use as needed, provided it is followed by the original. The variations between jurisdictions are confusing and costly, supporting this simple innovation would quickly change the way we communicate with customers and provide one of the many modifications that the market demands.

To answer the questions that arise in advance of launching electronic proof of insurance we can draw upon the experiences of the 43¹ jurisdictions in the United States where the technology is widely used. TD Insurance's comments in response to the questions in the CCIR's issues paper follow.

Privacy

In the U.S. when drivers hand their phones to law enforcement officers during traffic stops, they are doing so for the sole purpose of providing proof of insurance – any other information that is accidentally viewed or accessed intentionally or unintentionally cannot be used against the driver. TD Insurance supports a similar approach in Canada. Insurers can provide electronic proof of insurance via secure applications that may be programmed to block alerts from other applications running on the phone, protecting the privacy of drivers who choose to use electronic proof of insurance during interactions with law enforcement.

Law enforcement officers confiscating electronic devices if the validity of the electronic proof of insurance is in doubt seems unnecessary and would introduce a new set of liability and privacy issues while the device is in the officer's possession. It would be more appropriate for law enforcement to use the other punitive actions available – issuing tickets or laying charges related to false proof of insurance as they do now in response to pink slips that appear to be forgeries.

Liability

Mobile devices are increasingly fragile and expensive, ideally liability would be removed from the proof of insurance transaction by providing law enforcement with their own devices that they could use to scan – and perhaps authenticate – electronic proof of insurance when provided during a traffic stop. Since it's likely that this will not be the case at the outset, law enforcement should be protected from responsibility for any damage that occurs during the proof of insurance transaction and drivers should be made aware that they hand over their devices at their own risk.

Other Issues

Defining "reasonable inspection" with respect to electronic proof of insurance is a challenge that may be best left to the regulators, but the ideal transaction would involve the lowest risk of exposing any of the driver's personal information to the officer. Is it absolutely necessary for the officer to take both the driver's licence and proof insurance to his or her vehicle during a traffic stop? Can the necessary information be obtained by showing the officer the electronic proof of insurance and handing over the

¹ "Policymakers Take Positive Steps in 2015 to Modernize Insurance Laws" <http://www.pciaa.net/industry-issues/e-commerce>

driver's licence? Whatever the definition, it should be one that strikes a balance between protecting privacy and minimizing liability while meeting law enforcement requirements.

Travel between Canadian jurisdictions where one or more aren't yet accepting electronic proof of insurance will present challenges for drivers and law enforcement. As an insurer with customers across the country, TD Insurance looks forward to seeing a coordinated launch of the new technology in all Canadian jurisdictions led by the CCIR.

To avoid situations where drivers are unable to access their electronic proof of insurance, insurers can provide the document so that it resides on their customers' phones rather than being accessed via the internet, this eliminates the need for a network connection. Further, insurers and regulators can support drivers with education on the importance of ensuring they are prepared to provide proof of insurance during traffic stops, including the option to print a back-up copy that can be used if and when technology fails.

If electronic proof of insurance is provided in a format where it resides on a customer's phone, it may be possible to share the document amongst multiple drivers of the same vehicle. Insurers may choose a variety of methods to provide electronic proof: documents that can be saved locally, secure applications that house the documents and so on. While the technology has yet to be fully explored, there are opportunities to develop it to address the numerous privacy and access issues being discussed here.

As a back-up in case the technology fails, or in the event that a third-party is using an insured's car with permission but does not have access to a smart phone, insurance companies should be able to provide customers with the option to print their proof of insurance at home. In the event that printing proof of insurance at home becomes commonplace, adjustments will have to be made to the accepted format – pink slips may no longer be pink.

TD Insurance feels that the convenience of electronic proof of insurance should be made available to drivers of all classes of vehicles.

Using technology to deliver proof of insurance offers significant opportunities to reduce fraud. Delivering electronic proof through a secure application where customers must be authenticated to access the document will give insurers the opportunity to monitor and ensure legitimate use. Providing documents through an application rather than as standalone documents (a PDF or JPEG for example) will also make forgeries more difficult. Secure applications may also provide the added benefit of sharing electronic proof of insurance between multiple drivers of the same vehicle in a secure manner.

Supplementary Initiatives

TD Insurance agrees with the CCIR's suggestion that barcodes on electronic proof of insurance would make interaction between drivers and law enforcement easier, help to further reduce fraud, and increase privacy protection. TD Insurance would be pleased to participate in discussion on the topic and work together with regulators and law enforcement on this proposed innovation.

While this discussion is underway, TD Insurance would like to raise another solution for your consideration: an industry-wide database, accessible to and searchable by law enforcement to replace proof of insurance. No doubt this would involve some cost and significant coordination among regulators and the industry, but the rewards would far outweigh the investment. In many cases, law enforcement would likely be able to use existing tools to access the database during traffic stops to check whether drivers are insured. Most importantly, a database managed cooperatively by regulators and the industry would eliminate opportunities for fraud – without pink slips, paper or electronic, forgeries will disappear. Without the need for law enforcement to handle drivers' smart phones, issues of liability and privacy are also eliminated. TD Insurance believes this is a viable solution and looks forward to discussing it with the CCIR and industry partners.

Conclusion

TD Insurance is grateful for the opportunity to provide these comments on the Electronic Proof of Automobile Insurance Project Issues Paper from the Canadian Council of Insurance Regulator's Electronic Commerce Committee and wholeheartedly agrees with the recommendation to allow electronic proof of insurance in Canada. TD Insurance would be pleased to answer any questions on the content in this submission and to participate in further discussions on this topic.

Regards,



Nick Petter

Vice-President Customer Strategy, TD Insurance