City of Victoria - Privacy Impact Assessment

Plastiq Credit Card Payment Service

PIA #

Why do I need to do a PIA?

Section 69(5.3) of the *Freedom of Information and Protection of Privacy Act* (FOIPPA) requires the head of a public body to conduct a privacy impact assessment (PIA) in accordance with the directions of the minister responsible for FOIPPA.

Part 1 - General

Name of Department/Branch:	Finance		
PIA Drafter:	Rob Gordon / Christopher Paine		
Email:	rgordon@victoria.ca;	Phone:	**250.361.1347**
Program Manager:	Christopher Paine		
Email:	CPaine@victoria.ca	Phone:	**250.361.0396**

1. Description of the Initiative

The City will be cooperating with Plastiq to expedite the payment of property taxes by credit cards. Currently the City does not accept credit card payments for the property taxes at City Hall. Plastiq's payment service is available to their customers without the City's consent. A Plastiq customer may choose to pay his/her property tax bill by selecting the City as a Bill Payee. Plastiq will then forward the payment to City through already existing EDI payment services.

The City is cooperating with Plastiq to improve this service in 2 ways: (1) providing links to Plastiq's payment service on the City's website and (2) signing a preauthorized debit (PAD) agreement with Plastiq. The PAD agreement will facilitate payments from Plastiq directely into the City's bank account. Plastiq collects payments by credit cards and then will pay the City on the customers' behalf directly into the City's bank account.

To facilitate access to payment information, Plastiq will provide the City with a payment information portal. This portal can be used to review transactions and to determine which City accounts bulk Plastiq payments should be allocated to. It will also facilitate payment reversal.

2. Scope of this PIA

This PIA reviews the service Plastiq provides to residents and City staff.

3. Related Privacy Impact Assessments

This is a new service. There are no related privacy impact assessments.

4. **Elements of Information or Data**

Plastiq Registered Residents:

- First Name, Last Name
- Email address (optional)
- Phone number
- Credit card number
- City account number
- Type of payment
- Amount of payment
- IP address (obtained for fraud protection purposes only).

Personal Information city staff can access:

All of the above and Transaction IDs, Payments IDs, date and time of payment (e.g the transactional data).

The city only has access to the transactional data not the user specific information that is stored on Plastiq.com. City staff will not be able to access credit card numbers or IP addresses. The transactional data visible in the business portal does include email address as well as last 4 digits of credit card number and billing address zip code.

The question/form fields are configured uniquely for each merchant, to capture data elements required for attributing the payment appropriately (e.g. account number of the customer). By default, there are no question/form fields. Any questions/form fields need to be explicitly configured for each business, and will be visible to users on the Pay screen.

If personal information is involved in your initiative, please continue to the next page to complete your PIA.

If no personal information is involved, please submit Parts 1, 6, and 7 to your privacy office(r). They will guide you through the completion of your PIA.

Part 2 – Protection of Personal Information

5. **Storage or Access outside Canada**

   The server environment in Canada processes payments for both US and Canadian businesses (not exclusive to Canadian customers)

6. **Data-linking Initiative***

If you answer "yes" to all 3 questions, your initiative may be a data linking initiative and you must comply with specific requirements under the Act related to data-linking initiatives.	
1. Personal information from one database is linked or combined with personal information from another database;	no
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	no
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	no
If you have answered "yes" to all three questions, please contact your privacy office(r) to discuss the requirements of a data-linking initiative.	

7. **Common or Integrated Program or Activity***

If you answer "yes" to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.	
1. This initiative involves a program or activity that provides a service (or services);	yes
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	yes
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	no
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	

8. **Personal Information Flow Diagram and/or Personal Information Flow Table**

Personal Information Flow Table			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	Staff can view some personal information in transactional data	low	26(c)

9. **Risk Mitigation Table**

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	New personal information accessible on the City network	City has robust data protection measures	low	low

10. **Collection Notice**

Plastiq is a third party that allows residents to pay property taxes using their credit card. Except for your credit card number, the city does not collect additional personal information other than what it already collects to process payments by cheque, debit etc. Furthermore, the personal information will not be used or disclosed for any other reasons other than those uses and disclosures already

used to process payments by other payment methods. The legislated authority to collect your personal information is section 26(c) of the *Freedom of Information and Protection of Privacy Act.* For further information please contact Christopher Paine 1 Centennial Sq, Victoria BC V8W 1P6 cpaine@victoria.ca 250.361.0396.

Part 3 – Security of Personal Information

11. Please describe the physical security measures related to the initiative (if applicable).

Workstations are protected from public access by locked doors. Staff use access cards.

12. Please describe the technical security measures related to the initiative (if applicable).

Credit and debit card data is stored and managed in compliance with strict Payment Card Industry (PCI) standards. Plastiq utilizes tokenization, a payments industry-standard procedure. Your credit and/or debit card information is sent directly to our secure, encrypted data vault, which generates a random, cryptographically secure token that is used by our payment application to submit payments on your card. Once information is deposited into the vault, it cannot be directly retrieved by our payment application or any third parties. **Excerpted from Plastiq's Privacy Policy**

Access to user data is limited (e.g. via username/password authentication and 2-factor verification) only to those employees who require it to perform their job functions. Connections to this Website are secured with an Extended Validation (EV) SSL certificate with 256-bit encryption. Other security safeguards include, but are not limited to, encrypted vault storage for sensitive data.

13. Does your branch/department rely on any security policies?

Plastiq's security policies apply to protect the personal information on the servers.

14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

There are three default levels of access control.

15. Please describe how you track who has access to the personal information.

Changes to the data are tracked including Date/time of access, employee name, logout time, are they accessed (e.g. student tuition).

Part 4 – Accuracy/Correction/Retention of Personal Information

16. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If

personal information will be disclosed to others, how will the public body notify them of the update, correction or annotation?

The Plastiq Privacy Policy provides instructions to registered users.

17. **Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.**

    No

18. **If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.**

    N/A

19. **If you answered "yes" to question 17, do you have a records retention and/or disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?**

Part 5 – Further Information

20. **Does the initiative involve systematic disclosures of personal information? If yes, please explain.**

    No

21. **Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.**

    No

Please ensure Parts 6 and 7 are attached to your submitted PIA.

Part 6 – Information Access and Privacy Analyst's Recommendations

- Limit the use of Plastiq to the same use and disclosures of personal information as those currently
- Provide access to the Merchant portal to only those staff who currently process property tax

payments paid by cheque, cash, debit card etc.

- The Merchant Portal needs to have full audit capability to track staff who access it including what they accessed, changes made, where they accessed the portal from (if not at work), how long they were logged in and anything they may have downloaded, copied or printed.
- Confirm Plastiq complies with federal private sector privacy legislation.
- Employ the three access levels if staff don't all require the same level of access.
- If using the reports feature, aggregate personal information and do not create new reports containing personal information that are disclosed to staff that did not receive similar reports in previous years.
- What is the process for restoring forgotten passwords?
- Advise the Information Access and Privacy Analyst which access level staff will be given. Plastiq offers three different levels presumable based on need. Describe the access permissions of the level staff are provided.

Part 7 – Program Area Signatures

Rob Gordon	[signature]	May 8, 2015
Privacy Officer/Privacy Office Representative	Signature	Date
Christopher Paine	[signature]	May 8th/15
Program/Department Manager	Signature	Date
Contact Responsible for Systems Maintenance and/or Security (Signature not required unless they have been involved in this PIA.)	Signature	Date
Robert Woodland	[signature]	05/11/2015
Head of Public Body, or designate	Signature	Date

A final copy of this PIA (with all signatures) must be kept on record.