Part 1 – General Information

Name of Department/Unit	IT Services / Finance / Library Services	**Project ID**	2024-05
PIA Drafter	Kaitlyn Gutteridge		
Email	kgutteridge@ecuad.ca	**Phone**	778-833-0628
Project Sponsor	Sandeep Sidhu		
Email	sandeep@ecuad.ca	**Phone**	
Project Manager	Ali Entezari / Carlos Mendes		
Email	aentezari@ecuad.ca; cmendes@ecuad.ca	**Phone**	

1. What is the initiative?

OneCard by TouchNet is ECU's University ID card that provides student, staff and faculty (referred to herein as "user") access to library resources, A/V equipment checkout, and campus facilities, including classrooms, shops, studios, and any other areas and resources that are assigned for each user's specific requirements. Use of the OneCard VIP system has been in place at ECU for some time now.

One important functionality of OneCard is its ability to serve as a payment card for various merchants within the ECU campus. Instead of using a credit card or cash to pay for services, users can preload funds onto their OneCard and use it to process a payment. The potential use of this functionality is widespan – ECU has not leveraged this functionality to date and will be piloting OneCard's payment capability for printing services through the implementation of PaperCut's Payment Gateway Module (further described below).

The following section will provide a description of the major components assessed in this PIA:

1. OneWeb – web interface that permits users to interact with their OneCard account and add funds to their OneCard account using TouchNet's payment gateway.
2. PaperCut's Payment Gateway Module – the connection between PaperCut and OneCard servers that permits for funds to be transferred from OneCard to PaperCut.
3. U.Commerce Central – the centralized online portal that manages all university commerce system operations that are processed via TouchNet (including all OneCard and OneWeb transactions) and where authorized users can view commerce activity across campus.

OneWeb

Overview

OneWeb is the web interface that allows individuals to interact with their OneCard and add funds to their OneCard account (which are stored in the OneCard database). At this time, users can only access OneWeb within ECU's internal network; however, ECU is in the process of configuring an external IP for the webserver via EduCloud to authorize access from external networks, which is anticipated to be made available in early 2025. The OneWeb webserver communicates with the OneCard server/database (bi-directional data flows), and the OneCard database also feeds in information from Colleague (one-directional pull from Colleague to OneCard only).

ECU has entered into a payment processing agreement with TouchNet that permits ECU to utilize TouchNet's PCI compliant payment processing services (TouchNet's payment gateway) to facilitate the processing of credit card transactions via OneWeb. As such, ECU users can login to OneWeb and add funds onto their OneCard account and use them at applicable ECU merchants.

Data Flow

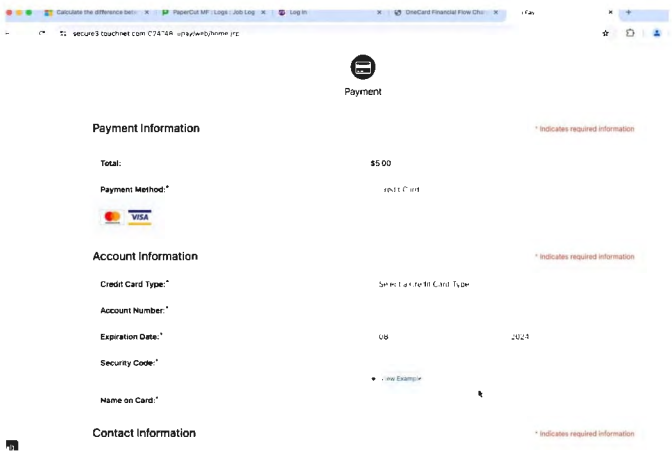
In terms of users' access to and engagement with OneWeb:

1. The ECU user logs into the OneWeb website via ECU's SSO and MFA. Once access is authorized, in the OneWeb platform the users can:
    a. Add funds to their OneCard and review their balance
    b. Deactivate their account in the case of a lost / stolen physical OneCard

    It is anticipated that OneWeb will offer additional user functionalities in the future as new ECU merchants are added to OneCard's payment offerings (e.g., parking pass payment; locker rentals).

2. Where a user intends to add additional funds, they proceed to the "Add Cash" option and the user is taken to a TouchNet-hosted payment processing landing page to process the transaction.

Figure One: TouchNet Payment Processing Landing Page

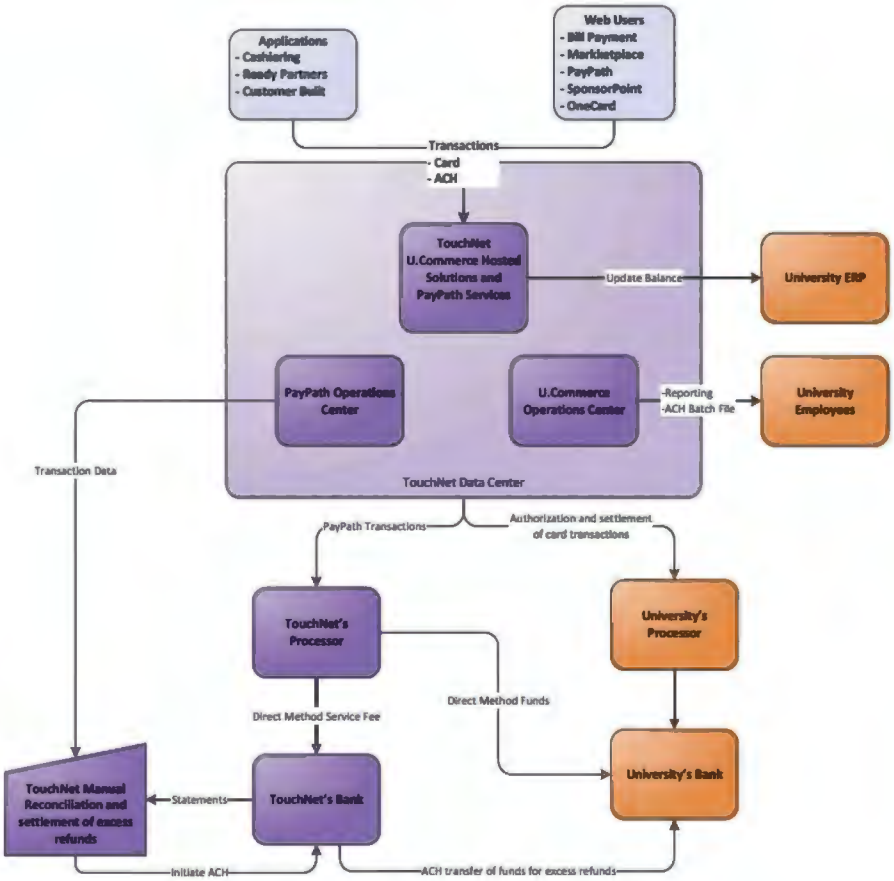


3. The user enters their credit card information and submits their payment; TouchNet sends the authorization request via the TouchNet payment gateway, and then sends all required data entered into the landing page to the credit card processor over a secure IP connection. The credit card processor approves the payment transaction on behalf of the bank that issued the card account. When the credit card processor responds with an authorization, rejection, or error, the TouchNet system logs the response to the payment gateway database and sends the response back to the payment application.

   Where the transaction is successful, TouchNet's payment processing database submits a confirmation token back to ECU's OneCard server/database confirming the transaction and transaction amount, and the updated balance is added to and stored in the OneCard database. The user will view the transaction and updated balance via OneWeb (similar to a bank transaction).

   At no time during the transaction is any credit card information accessed, processed, or stored by ECU, rather TouchNet's payment gateway acts as a third party for processing the credit card payment and hosts the infrastructure and systems to process the credit card payment. TouchNet has achieved PCI compliance as a Level 1 Service Provider, and it is compliant with the PCI Data Security Standards (PCI-DSS) and the PCI Software Security Framework (PCI-SSF). Furthermore, users will not be permitted to store credit card information for future payments in the TouchNet payment processing landing page.

Figure Two: Overview of TouchNet's payment processing options / processes



PaperCut

Overview

PaperCut is a software application designed to help organizations manage printing. PaperCut works by intercepting print jobs as they pass into a print queue. It watches the queues and extracts job information such as page counts and uses this to implement:

- Logging, charging, control, quotas, reporting or a combination of all.
- Security features like secure print release, archiving and watermarking.

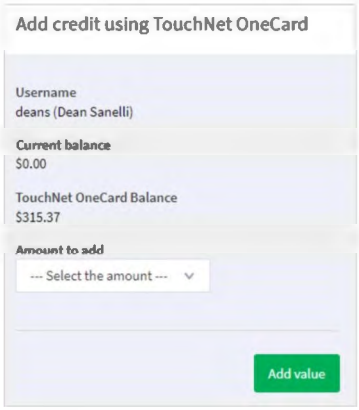
The PaperCut technical components (servers and databases) are hosted on ECU's EduCloud and any data PaperCut transmits between system components is encrypted. Given PaperCut has been in use by ECU for many years, a comprehensive assessment of PaperCut will not be completed in this PIA and additional details about the day-to-day use and administration of PaperCut at ECU can be found here.

For this PIA, what is new to ECU's use of PaperCut is the installation of PaperCut's Payment Gateway, a feature that allows value to be transferred from an external system to a PaperCut personal account. Payment providers such as TouchNet/OneCard support the concept of pre-stored or pre-authorized value which allows PaperCut to transfer value with or without user intervention at the time a job is being charged. For the purposes of processing a printing job using PaperCut, ECU has installed and configured the PaperCut Gateway Payment Module, which connects the PaperCut server/database to OneCard server/database. All PaperCut components and the Gateway Payment Module are also hosted in ECU's EduCloud environment and been configured in accordance with ECU's Information Security policy and standards.

Data Flow

1. When the user accesses a printer to release a print job, the user can tap their OneCard and PaperCut will first check if there are any funds in the PaperCut account. If so, PaperCut will use these, and if not, it will pull from OneCard.
2. Where a user logs into the PaperCut online portal to manage their account and jobs, the user can also manually transfer funds from OneCard to PaperCut account (this manual transfer will be decommissioned in the future).

Figure Three: Example of PaperCut Transfer from OneCard

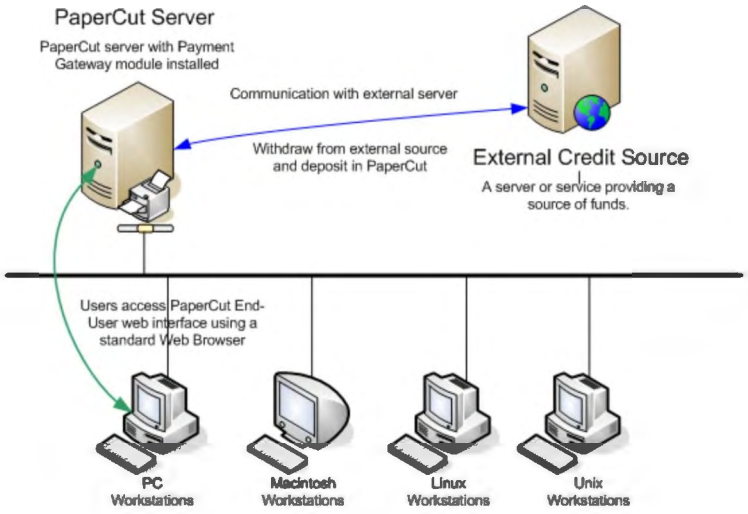


3. Where the funds are transferred from OneCard to PaperCut, PaperCut is simply interacting with the OneCard server as PaperCut receives a token back from OneCard server saying that funds are available or not available in the OneCard database. Where funds are available, they are transferred to the PaperCut database and up-to-date balances are reflected in both databases. At no point does PaperCut redirect to a separate payment portal or process any credit card information, rather it only adds value from the OneCard account if the user has funds available.

   To map users between PaperCut and OneCard databases, ECU will employ the user's OneCard number as the unique ID. The OneCard number is a distinct number provided on each physical

OneCard and is a random string of numbers that is not linked to the user's personal information. The OneCard number will be stored in both databases.

Figure Four: Overview of PaperCut Payment Gateway Module



4. In the case where there are not sufficient funds in OneCard to transfer to PaperCut, users must either:
   a. Add more funds to the OneCard account via OneWeb to update their account balance (and can manually pull them to PaperCut or retain them in OneCard), or
   b. As per the standard process in place at this time, add more funds in person via cash by interacting with authorized cashiers on-site. These funds are deposited directly by the cashier to the user's PaperCut fund via PaperCut's online account management site and cannot be pulled back to the OneCard account. Previously, cashiers facilitated payment card transactions as well, but given the move to OneWeb, cashiers will be limited to cash transactions.

U.Commerce Central

Overview
U.Commerce Central is a centralized location to manage U.Commerce system operations, view commerce activity across campus including OneWeb and OneCard, and access the U.Commerce Central help system. It's the "command center" for campus-wide financial and user management and encompasses all of ECU's TouchNet campus solutions. U.Commerce Central permits ECU to:

a. View all commerce activity for a particular date range.
b. Identify and take action on issues requiring financial oversight.
c. Reconcile monthly, quarterly and yearly transactions and process refunds.
d. Access any TouchNet administrative applications with a single click.
e. Manage users, passwords, and login policies.

.
U.Commerce Central is also hosted within EduCloud and forms part of ECU's TouchNet / OneCard systems architecture. In comparison to OneWeb, SSO is not configurable with U.Commerce Central and a separate username, password and MFA are required for access. Authorized ECU administrators oversee provisioning and deprovisioning user accounts, assigning passwords, assigning user roles and privileges, auditing activities and configuring system controls. At the time of writing, ECU IT and Finance staff were in the process of developing policies and processes to oversee activities within U.Commerce Central.

2. What is the scope of this PIA?

In scope

- Implementation of OneCard web interface and TouchNet payment processing services, which permits users with a OneCard to add funds to their OneCard for use within various ECU merchants.
    - This PIA is currently limited to PaperCut, but ECU is investigating the option to expand to other merchants. Where ECU adds new merchants, an amendment to this PIA will be completed to discuss the new use case.
- Implementation of PaperCut Payment Gateway Module, which authorizes PaperCut to pull funds from OneCard to the user's PaperCut account to pay for print jobs.
- Implementation of TouchNet's U.Commerce Central for use by ECU's Finance and IT departments.

Out of scope

- Initial set up, configuration and use of OneCard VIP System by ECU to date.
- Initial set up, configuration and use of PaperCut by ECU to date, including processes in place for cashier support to complete payments / top-ups for PaperCut accounts.

3. What are the data or information elements involved in the initiative?

Information collected and processed by the TouchNet payment gateway for processing credit card transactions

- First and Last Name
- Credit Card Account Number, Expiry Date, and Card Security Code
- Billing Address

Information collected and stored by ECU in the OneCard database

- ☐ ECUAD ID Number
- ☐ OneCard Number
- ☐ First and Last Name
- ☐ Preferred Name
- ☐ Designation
- ☐ Start and End Date
- ☐ Home Address (to process any account refunds via cheque)
- ☐ Account Balance
- ☐ Transaction and Account History
- ☐ OneCard Photo

Information collected and stored by ECU in the PaperCut database

- ☐ First and Last Name
- ☐ OneCard Number
- ☐ Account Balance
- ☐ Print Job History

Information presented on OneWeb web interface:

- First and Last Name
- OneCard Photo
- ECUAD ID Number
- Account Balance
- Transaction and Account History

Information presented in U.Commerce Central

- Records of all transactions completed by ECU users using TouchNet services (OneCard; OneWeb), which may include:
  - User's First and Last Name
  - OneCard Number
  - Transaction and Account History

4. Does the initiative include personal information?

Yes, see list above.

Part 2 – Collection, Use and Disclosure

This section will help you to identify the legal authority for collecting, using, and disclosing personal information and to confirm that all personal information elements are necessary for the purpose of the initiative.

Use this column to describe the way personal information moves through the initiative step by step as if you were explaining it to someone who does not know about your initiative.	**Collection, use, disclosure**	**FOIPPA authority**
1. User logs into OneWeb via ECU SSO and MFA to either (1) suspend OneCard or (2) "Add Cash" to OneCard account.	Collection	26(c)
2. Where the user decides to "Add Cash", the user submits their credit card payment information via the TouchNet payment processing landing site.	Collection, Use	26(c); 32(a)
3. TouchNet processes payment information via its PCI DSS compliant payment gateway and infrastructure, and submits confirmation token to ECU.	Use, Disclosure	32(a); 33(2)(u)
4. ECU stores updated OneCard balance in OneCard database and user can view funds via OneWeb.	Collection, Use	26(c); 32(a)
5. User uses OneCard to pay for printing job either by tapping their card at the printer or manually moving funds from OneCard to PaperCut. Both actions are supported by the PaperCut Payment Processing Gateway.	Use	32(a)
6. Authorized ECU staff review and reconcile transactions and complete required financial activities via U.Commerce Central. ECU staff login via login credentials and MFA to complete the required actions.	Use, Internal Disclosure	32(a); 33(2)(h)
7. TouchNet stores payment processing information in PCI DDS compliant datacentres in USA until the termination of the contract.	Storage; Retention	30; 31
8. ECU securely stores all OneCard, OneWeb, and PaperCut information in EduCloud in accordance with ECU's records retention schedule.	Storage; Retention	30; 31
9. TouchNet uses users' information for the purposes of maintaining, troubleshooting, and repairing the system.	Use, Disclosure	32(a); 33(2)(t)

5. Collection Notice

An updated Privacy Notice and Terms of Use for OneCard that includes the use of OneWeb were both Under development at the time of writing. The updated Terms of Use will consolidate previous Terms drafted for OneCard, OneCard photo upload, and OneWeb into one document. The following FIPPA Collection Notice will also be presented alongside the Terms of Use.

Emily Carr University (ECU) provides services offered by TouchNet including OneCard and OneWeb to permit ECU students, staff, and faculty access to library resources, A/V equipment, and campus facilities. ECU also permits you to upload funds to your OneCard to use at applicable ECU merchants. Where you decide to add funds to your OneCard via OneWeb, ECU employs TouchNet's payment processing services to process the credit card transaction. Your credit card information will be securely processed and stored by TouchNet in the USA within PCI DSS complaint infrastructure.

The personal information you provide when accessing and using TouchNet services for the purposes outlined above is collected by ECU under section 26(c) of the B.C. Freedom of Information and Protection of Privacy Act.

If you have any questions about the collection, use, and disclosure of your personal information, please contact Emily Carr University's Privacy Office: privacy@ecuad.ca.

TouchNet also provides a Privacy Notice within the OneWeb portal that describes TouchNet's activities in relation to information that is processed and stored by TouchNet when engaging in credit card transactions.

Part 3– Storing Personal Information

6. Is any personal information stored outside of Canada?

EduCloud

All servers, databases and supporting technical infrastructure for TouchNet (OneCard, OneWeb) and PaperCut (including the Payment Gateway Module) will be hosted on ECU's EduCloud instance. A PIA has been completed for EduCloud, and EduCloud is currently used by ECU to various software and service solutions in support of ECU's operations. A brief overview will be provided below[1] and more information about EduCloud is available here.

EduCloud is a virtual data centre for B.C.'s higher education institutions that is operated and supported by the University of British Columbia. This private, self-managed cloud server service offers simple and secure access to provision and manage virtual servers at a fraction of the cost of implementing physical servers. The service is available 24/7, is fully monitored, and is FIPPA compliant, securely storing all data within British Columbia (physical infrastructure located in Vancouver and Kamloops). EduCloud offers

[1] https://www.bc.net/service-catalogue/shared-systems-and-technology/educloud-server

secure, multi-tenant infrastructure as a service. ECU is supplied with isolated virtual pools of compute, storage and network resources, which can be used to build and deploy robust, highly available applications and services for the institution. It is built using VMware vSphere technology, the industry-leading server virtualization platform.

TouchNet Payment Processing Services
Where credit card payments are processed using TouchNet's payment gateway, credit card information will be processed and stored in TouchNet's PCI DSS complaint datacentres located in continental USA. These datacentres are hosted by a third-party, QTS.

7. Where and how are you storing the personal information involved in the initiative?
See Question 6 above.

8. Does the initiative involve sensitive personal information? If yes, where and how are you storing the personal information involved in the initiative?
Credit card information will be collected, processed and stored by TouchNet for the purpose of facilitating users' credit card transactions.

Part 4 – Assessment of Disclosure Outside of Canada

Complete this section if you are disclosing sensitive personal information to be stored outside of Canada. Otherwise continue to Part 5.

9. Is the sensitive personal information stored by a service provider?

If yes, fill in the table below (add more rows if necessary)

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where and how is the sensitive personal information stored (including backups)?
1. Global Payments, parent company representing TouchNet for the purposes of the payment processing agreement	N/A	QTS datacentre, a service provider to Global Payments. Physical location of QTS datacentres is located in continental USA.

10. Describe the contractual terms in place (if applicable).

ECU has entered into a contract with Global Payments for *Payment Card Processing Services and Equipment*. Global Payments is the parent company of TouchNet and represents TouchNet in the contract executed for the payment processing services, specifically the use of TouchNet's payment gateway to process credit card transactions for the purpose of adding funds to users' OneCard accounts.

Canadian-specific privacy protections are included in the contractual provisions, but the FIPPA Privacy Protection Schedule was not included during the execution of the contract. The contract holds a three-year term.

11. Are you relying on an existing contract, such as an enterprise offering from BCNet?
No, we are not relying on an existing contract.

12. What controls are in place to prevent unauthorized access to sensitive personal information?
The following controls are in place to prevent unauthorized access to sensitive personal information:

- Contractual controls in the form of an executed contract between Global Payments and ECU that outlines Global Payments obligations to the protection of personal information including implementation of appropriate technical and organizational measures to protect personal information, breach notification, ongoing external audits / certifications.
- External certifications obtained by TouchNet to demonstrates its privacy and security compliance – SOC 2 Type II and SOC 1 Type II certifications, PCI Level 1 Service Provider, and are compliant with the PCI Data Security Standards (PCI-DSS) and the PCI Software Security Framework (PCI-SSF).
- The following are among the security measures employed by TouchNet:
    - Administrative access to TouchNet's datacentres is restricted. A limited number of TouchNet's staff can access products installed in its datacentres and separation of duties is enforced.
    - TouchNet products use industry-standard methods to protect sensitive payment data. This includes masking sensitive payment data presented to the end user. All account numbers and other highly sensitive data are stored with strong cryptography as defined by PCI DSS. Such data is also protected during transmission over public networks using PCI-DSS compliant cryptography. All external backups utilize full drive encryption
    - TouchNet monitors systems hosted by TouchNet 24x7 and limits physical access to the systems to only those individuals that must have access. Physical access is also monitored by TouchNet staff.
    - TouchNet performs routine scans on its networks and applications to locate any potential vulnerabilities.
    - Sensitive data used to troubleshoot issues is isolated to segregated terminal machines. TouchNet also performs routine scans of staff machines to verify that no sensitive data is present on workstations.
    - All applications are subject to code review prior to implementation.
    - TouchNet maintains firewalls that comply with all PCI DSS requirements such as "deny all" configuration, formal configuration standards, periodic review, etc.
    - The application is protected against commonly used hacker techniques such as SQL Injection or Cross-site scripting, and other vulnerabilities listed in the OWASP (Open Web Application Security Project) Top Ten.

13. Provide details about how you will track access to sensitive personal information.
TouchNet has validated their datacentres for PCI DSS compliance and has completed a SOC 1 Type II audit and SOC 2 Type II audit. TouchNet employs industry-leading security incident and event log

management systems to store, restrict access to logs, and correlate events. Per PCI DSS, TouchNet is required to log user activity within each application. Activity is logged and maintained for at least 12 months. Some such activity may be reported and presented in the application while other such information is stored only in back-end system logs that TouchNet personnel can review.

14. Describe the privacy risks for disclosure outside of Canada?

Privacy risk	Impact to individuals	Likelihood of unauthorized collection, use, disclosure, or storage	Level of privacy risk (low, medium, high)
Privacy laws in USA, including the Patriot Act, and specific states whereby the data will be stored, processed and backed up, do not provide equivalent personal information protection controls and access rights as FIPPA	Medium	Low	Medium
Risk response (this may include contractual mitigations, technical controls and/or procedural and policy barriers) ▪ Contractual controls already in place for Canadian compliance; Global Payments to comply with FIPPA privacy protection schedule for service providers. ▪ Limited information stored in the USA and enhanced physical, network and administrative controls in place as validated via PCI DDS compliance, SOC 1 and 2 audit reports. ▪ Users are notified that their credit card information will be processed and stored in the USA. If they do not want to proceed, have the option of adding cash to their account via cashiers.			
Is there any outstanding risk? If yes, please describe. Minimal outstanding risk will be present with the implementation of the mitigations described here.			

Part 5 – Security of Personal Information

15. Does the initiative involve digital tools, databases, or information systems? Yes / No

Yes, it involves EduCloud, TouchNet (OneCard, OneWeb, U.Commerce Central) and PaperCut databases and digital infrastructure.

16. Do you or will you have a security assessment to help you ensure the initiative meets the reasonable security requirements? Yes / No

Yes, for EduCloud's security controls, please see description in Question 6 and for TouchNet's security controls for the purposes of payment processing, please see below.

TouchNet's payment platform is PCI Validated Payment Software as well as compliant with PCI DSS, PTS including EMV certification. TouchNet has validated their Data Centers for PCI DSS compliance and has completed a SOC 1 Type II audit and SOC 2 Type II audit. TouchNet employs industry-leading security incident and event log management systems to store, restrict access to logs, and correlate events. TouchNet has submitted an up-to-date HECVAT and copies of its SOC 1 and SOC 2 reports for ECU's review and analysis.

17. Controlling and tracking access - Please check each strategy that describes how you limit or restrict who can access personal information and how you keep track of who has accessed personal information in the past. Insert your own strategies if needed.

Strategy	Yes / No and please describe
We allow employees only in certain roles access to information ECU Access to the OneCard and PaperCut databases are limited to authorized ECU employees only with least privilege and need to know controls in place. For the U.Commerce platform, IT and Finance are developing a RACI matrix and associated roles and privileges in accordance with the fine-grain access controls offered by the U.Commerce site. This approach was in development at this time and will be further refined as roles are assigned to oversee TouchNet and its associated services (OneCard, OneWeb, U.Commerce). At the time of writing, it was noted that the current resourcing model for supporting these services was not sustainable and a long-term solution for providing oversight in the sustainment phase required further consideration by ECU. TouchNet One TouchNet representative has access to the U.Commerce platform for administration and troubleshooting purposes.	Yes
Employees that need standing or recurring access to personal information must be approved by the appropriate authority ECU IT and Finance currently oversee administrator rights for the various TouchNet systems, and user roles and privileges must be generated via IT and Finance administrators.	Yes

TouchNet One TouchNet representative has been authorized by TouchNet and ECU to access to the U.Commerce platform for administration and troubleshooting purposes.	
We use audit logs to see who accesses a file and when ECU Logging and monitoring controls are in place for all systems at this time (OneCard, OneWeb, U.Commerce, PaperCut) and audit logs are available for review in the systems. However, no proactive monitoring and auditing protocol specific to the various systems, outside of standard EduCloud security and infrastructure monitoring, is in place at this time. Given resourcing concerns, it is anticipated that retroactive auditing will be adopted at this time. For U.Commerce, administrators can review user history directly in the platform. The "History" window displays a list of a user's permissions, tasks performed, and messages about user authentication and account activity in U.Commerce Central. TouchNet Access by the TouchNet administrator to U.Commerce is logged but no proactive monitoring and auditing protocol specific to the administrator's activities is in place at this time.	Yes
Additional strategies:	N/A

Part 6 – Accuracy, Correction + Retention

In Part 6 you will demonstrate that you will make a reasonable effort to ensure the personal information that you have on file is accurate and complete.

18. Do you have a process in place to correct personal information?
Processes are already in place with OneCard and PaperCut for users to update their information, including updating names on a user's OneCard, and requesting PaperCut refunds. Additional options for requesting refunds from a user's OneCard will be included on ECU's websites and the revised Terms of Use.

19. Does your initiative use personal information to make decisions that directly affect an individual(s)?

No – the initiative does not use personal information to make a decision that directly affects an individual.

20. Do you have a retention schedule in place related to personal information used to make decisions? 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?

No information will be used to make a decision about an individual. In general, information stored in PaperCut and OneCard databases that are in the custody and control of ECU will be retained and destroyed in accordance with ECU's records retention schedule.

In accordance with the *Payment Card Processing Services and Equipment Contract*, Global Payments (representing TouchNet) will delete or return any personal information at the end of the contract and delete any remaining copies. Global Payments may be required to retain certain aspects of personal information if needed to comply with applicable law or for insurance, accounting, taxation or record keeping purposes. Any personal information that Global Payments retains under this requirement will be maintained subject to the protections in the *Payment Card Processing Services and Equipment Contract*. However, in the event the ECU would like a copy of its data, beyond what it had access to during the contract term, TouchNet will work with ECU to find a mutually agreeable solution based on the needs of ECU and the industry standards at the time of the termination.

Part 7 – Additional Risks

Possible Risk	Response	Risk Level
Risk 1: While the *Payment Card Processing Services and Equipment Contract* considers contractual obligations to comply with Canadian legislation, mainly PIPEDA, no specific FIPPA obligations are detailed. Given credit card information will be stored outside of Canada, ECU must ensure that Global Payments / TouchNet complies with FIPPA obligations for the processing and storage of personal information (i.e., credit card information) outside of Canada. Users must also be made aware of this scenario prior to submitting credit card information. .	The FIPPA Privacy Protection Schedule must be agreed to by Global Payments and appended to the contract. Additional information about processing outside of Canada must be included in the Privacy Notice (see draft Notice above with USA specific language).	Medium

Possible Risk	Response	Risk Level
Risk 2: Given the expanded services provided by ECU with this initiative, updated terms and conditions must be made available to ECU users to ensure the appropriate and acceptable use of OneWeb, OneCard and PaperCut. Users must also be sufficiently informed of the privacy controls in place to protect their personal information, and as mentioned in Risk 1, processing of credit card information outside of Canada.	Updated Terms of Use and Privacy Notice to be finalized and posted on the ECU website. Users to receive email notification of these updates once available (consider mass ECU email blast). Kaitlyn Gutteridge to support project team in finalizing this documentation in time for the anticipated launch (mid-January 2025).	Medium
Risk 3: Given the human resourcing requirements needed to implement the new systems (U.Commerce Central and OneWeb) and updated systems (OneCard and PaperCut), a sustainment plan must be in place to ensure systems are sufficiently supported and managed both from a technical and administrative standpoint moving forward. If not, this could potentially lead to unauthorized collection, use and disclosure of personal information. At the time of writing, no specific project manager had been designated to oversee this work long-term.	Carlos Mendes has drafted various data flows and responsibility flows to describe the departmental oversight and positions required to support the service provision; additional follow up and confirmation of these models must be completed. ECU to appoint a project manager to oversee the long-term sustainment model of these integrated systems along with the vendor relationship with TouchNet.	Medium
Risk 4: Additional details were requested from TouchNet about the physical location of the QTS datacentres in the USA. This information was not provided to ECU in time for drafting the PIA and TouchNet responded noting that they were quite busy, and it would take some time.	ECU to update PIA once TouchNet provides specific geographical information about the QTS datacentres in the USA. ECU to determine if specific SLAs are required for managing the relationship with TouchNet to ensure time-sensitive risks are communicated and mitigated.	Medium

Possible Risk	Response	Risk Level
Given ECU has experienced many delays in receiving information from TouchNet, there is concern that this could result in the future delays when receiving time sensitive information (e.g., breach notification).		

Please ensure Parts 7 and 8 are attached to your submitted PIA.

Part 8 – Program Area Signatures

This PIA is based on a review of the material provided to the Privacy Office as of the date below. If, in future any substantive changes are made to the scope of this PIA, a PIA Update must be completed and submit it to Privacy Office.

Department Manager	Signature	Date
Sandeep Sidhu *Chief Information Officer*	Signature	19 Dec 2024 Date
Adrian Tees *Privacy Officer*	Signature	January 7, 2025 Date

A final copy of this PIA (with all signatures) must be delivered to privacy@ecuad.ca for record keeping.