Payment Card Processing – Swipe Terminal vs. Web

Financial Area:

Vice President for Finance

Responsible or Contact Office/Role:

Financial Reporting & Operations (Payment Card Services)

Review Date:

January 14, 2019

Swipe Terminals:

Typically, swipe terminals are used for face to face/card present transactions. Or, a terminal is used to key enter Mail Order or Telephone Order transactions where your customer is registering for an event or function of some kind and the department does not have a website that accepts registrations or payments. A swipe terminal is the most secure method of transmitting cardholder data and the cost of the machine is minimal, see below. The primary security issue with swipe terminals is protecting the customer's account number from misuse on paper forms and from misdirection by the person in possession of the customer's card.

VeriFone VX 520 – Desktop Swipe Verifone resource Documents	**$ 495.00 – no tax**
Verifone Vx820 Pin Pad	**$ 225.00 – no tax**
Ingenico ICT 250 – Desktop Swipe Quick Start Guide	**$ 365.00 – no tax**
Ingenico iPP Pin Pad 320	**$300.00 – no tax**
VeriFone MX 915 **Setup**	**$566.00 – no tax, plus $ 20.00 Sims Card and $19.00 monthly line maintenance per terminal (battery or plug-in).**
Poynt WiFi Smart Terminal	**$999.00 – no tax, plus $29.99 monthly**

There are two types of swipe terminals, desk-tops that are hard-wired into an analog phone line and cellular terminals that use the cellular network to communicate to the card processor. Cellular terminals can also plug into an analog phone line and be used as a conventional swipe terminal. Cellular machines can be as mobile as Mobile and can operate off of a battery for up to 10 hours. They will also accept Chip cards, Debit PIN transactions and tap-and-go Smart Phone transactions.

Once the application for a new swipe terminal account is approved, the terminal itself will be shipped directly to your physical address and delivered by UPS. The cost of the terminal will be reflected on your first Elavon statement and will be included in the monthly fees that are billed to the PTAO that was provided on your application.

For information on borrowing a wireless swipe terminal for special events, see
Borrowing Cellular swipes terminals for Special Events.

Terminal Usage and Security

The first video will demonstrate the security issues with swipe terminals and the second will demonstrate the varied ways that the face-to-face cardholder transactions are completed.

Videos

https://www.youtube.com/watch?v=R8dQo-hrlR4&feature=youtu.be This is a Canadian video about swipe card security. Do not expect to receive the $100.00 reward.

https://www.youtube.com/watch?v=G_cURYerH8k How to process payments using EMV terminals with chip and PIN or Contactless with a Mobile Wallet.

Guidance Documents
https://www.campusguard.com/public/NewsArticle-2018.11.20-DeviceInspectionGuide.pdf
A good step by step guide on inspecting your swipe devices.

Terminal Obsolescence

Elavon will take terminals in-trade for a newer model as long as the device is still PCI Compliant and you have purchased the equipment through them. The difference will be billed along with the monthly fees on your statement from Elavon to the department's PTAO. Place the order for a new machine from the PCS (Payment Card Services, 4-4362).

If you are terminating a swipe account or the terminal is no longer supported by Elavon then there will not be any rebate. Please dispose of the equipment through Procurement's surplus property program.

SAQ B Requirements for Swipe Terminal operations

Requirements 3, 4, 7 and 9 all address the physical security of cardholder data, the PAN (account number), security code, expiration date and Cardholder name and the policies that govern the security:

- who has access,
- what access to they have and is it necessary,
- how and what is stored,
- no data through emails,
- how data is stored, tracked and destroyed,
- is the swipe devise kept secure, examined and guarded against tampering and tracked. Use the Inventory Log document to track the secure status of a swipe device.

Requirement 12 addresses institutional policies on information security, third-party contracts and compliance and incident response plans.

Website requirements and design:

Website development and design is a departmental responsibility. Typically, the website will supply information about the event or product. The department can also opt to collect registration information on their site, process this information and provide reports to the department. The application must NOT capture, store or transmit the actual credit card number – this function is managed through the website's connection to either the University Gateway (E-Pay @ UVA) or an approved third-party's gateway provider to insure cardholder security and PCI compliance.

- University Gateway through Nelnet (EPAY @UVa/Commerce Manager) can provide a limited front-end information gathering/registration page and a secure payment page hosted by Nelnet for an additional fee of $.30 per transaction for the use of the Gateway plus regular processing fees.

- Third-party software solutions: These products are known as "Payment Applications" (PA-DSS) and the vendor is known as a "SERVICE PROVIDER". Refer to Third-Party Service Provide Guidance and the Application for a Third-Party Service Provider Payment Card Solution. Payment Applications usually provide a myriad of option for reporting, sorting, or manipulating the data that you collect from your customer. They may also provide credit card processing as part of the package. Please contact the Payment Card Services early in your decision making process to avoid unnecessary delays. We can help you understand the compliance issues and assist you with the Procurement and the contractual issues that arise with these types of negotiations. The PCI Standards guidance document on Third-Party providers can be found at:

  https://www.pcisecuritystandards.org/documents/PCI_DSS_V3.0_Third_Party_Security_Assurance.pdf

  The fees associated with a third-party are borne by the department and can be quite expensive. The set-up and interfaces require review *by Information Security, Policy and Records* and/or the University's Qualified Security Assessor (QSA – CampusGuard). In addition to the third-party fees, there are also regular credit card processing fees. See Costs and Fee on this website.

If the web page is managed locally, there is a University requirement for a "Landing Page" where the "Pay Now" button resides. *PCI Standards require that the Landing Page reside on a PCI compliant server. The department will work with CACS (Custom Applications & Consulting Services) here at the University in order to link that page to either a Microsoft AZURE server or Amazon ACQUIA server before the department will be allowed to accept payment cards.*

Our processor Elavon also requires that the website or Landing page provide the following information:

- Doing Business As name prominently displayed;
- Contact information – C/S phone or email;
- Address for customer correspondence;
- **Country of establishment (**see *Note*);
- Return/Refund policy and location;
- Delivery method and timing;
- Multiple shipment policies (if applicable);
- Privacy policy statement;
- Product/Services including prices;
- Website order page secure;
- Domain registered – Pharmaceuticals only;
- Card brand acceptance marks (logos) displayed.
- The page where your customers' card information is entered must contain a valid SSL certificate

Note: As of August 2017, the card companies have required that "USA" be part of the merchant's address.
Disclosure of Merchant Location: must be "prominently and clearly disclosed to the Cardholder at all points of interaction". "The location (physical address) of the Merchant to enable the Cardholder to easily determine, among other things, whether the Transaction will be a **Domestic Transaction** or a **Cross-border Transaction**. The Merchant location must be disclosed before the Cardholder is prompted to provide Card information."

For EPAY users, the logical position for the full address that includes USA is on the Landing Page. For departments using a third-party vendor where the cardholder is passed to the payment page by the third-party, departments may have to include the address with the country on the pages preceding the handoff to the third-party. Or, we may have to negotiate with the third-party.

Elavon will provide a CONDITIONAL APPROVAL which means that we will receive a merchant account number and a list of the above requirements that need to be met. We can process payments on the merchant account but until the requirements have been met, NO DEPOSIT will post to the bank or your Clearing or Revenue project. If the CONDITIONAL APPROVAL drags on too long without the issues being resolved, Elavon may CLOSE the account with or without warning.

For more information and a sample of a Landing page, see "Website Requirements" under the PCI section.

The following web sites may assist the department with web site development for design, content and the do's and don'ts.

Guidelines for Web Design	https://brand.virginia.edu/tools-templates/web-design
Web Site Advertising	http://uvapolicy.virginia.edu/policy/IRM-001

If the department does not have the resources to build a web page or registration page on an existing web site, CACS – Custom Applications & Consulting Services, a part of ITC might be able to assist you. Please contact Custom Applications & Consulting Services at https://cacs.virginia.edu/contact for more information.

If your unit is interested in establishing a donor webpage or donor interface through your website and you do not have a development officer, contact University Advancement – Communications for assistance.