$ Payment Processing Paradigm $

Gail “Montreal” Shoffey Keeler

August 14, 2009

Agenda – Session Sections

- Introduction
- Payment Processing Basics
- Merchant Accounts
- Payment Card Industry Compliance
- Coding to Merchant APIs
- Questions

Ask Questions

INTRODUCTION

About Me – “Montreal”

- I am a born Quebecois
  - Permanent resident of USA
  - Passed the naturalization test last month
  - I will soon be sworn in as an American!
- Software Architect for AboutWeb
  - Contract at Social Security Administration
- BSIT, 2006
- MIS, 2008
- Working on DM/IST, estimate 2012
- Harley-Davidson riding fool!

2006 Ultra Classic Electra Glide

I have rode my bike across country several times – all by myself!

Target Audience

- Developers
  - Create eCommerce websites
  - Inherit an eCommerce website
- Analysts
  - Prepare requirements
  - Review eCommerce
- Managers
  - Understand the complexities and obligations of an organization to be PCI DSS compliant
  - Know the steps in bringing the organization into compliance.

The Basics

PAYMENT PROCESSING

Why Add Payment Processing?

- User
  - Uncomplicated and seamless purchasing experience
  - Savings in checks, postage, and envelopes
- Organization
  - Increase workplace efficiency
  - Increase security and reduction of errors
  - Eliminate lost or stolen checks
  - Improve cash flow for vendors
  - Improve timing and certainty of payments
  - Acknowledge receipt
  - Create and maintain satisfying customer relationships
  - Get paid in real time

Types of Electronic Payments

- Credit cards
- Instant transfer – debits
- eChecks
- Re-occurring / subscription
- Refunds
- PayPal accounts

What are the Processes?

- Authorization
  - Validate funds
    - Payments may be voided
- Settlement – Collecting Funds
  - Automated Clearing House (ACH) Network
    - Electronic checks are converted
    - Financial institutions exchange funds
    - Payments may not be voided, they must be refunded

Requirements

- Secure Socket Layer (SSL) Certificate
- Shopping cart
- Checkout / payment system
- Merchant account
- To ensure compliance with the Payment Card Industry (PCI) Data Security Standards

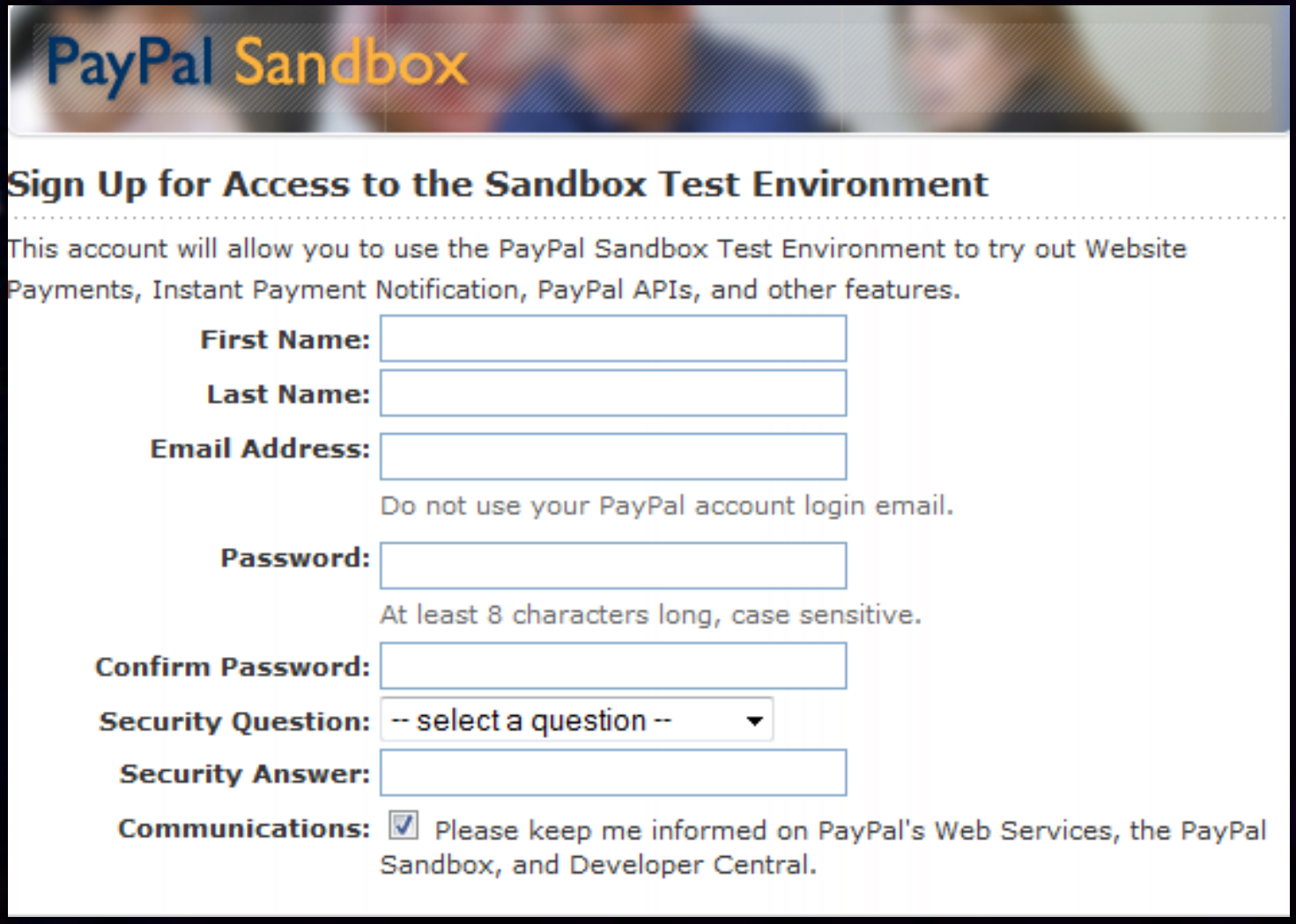
Example: Setting Up PayPal

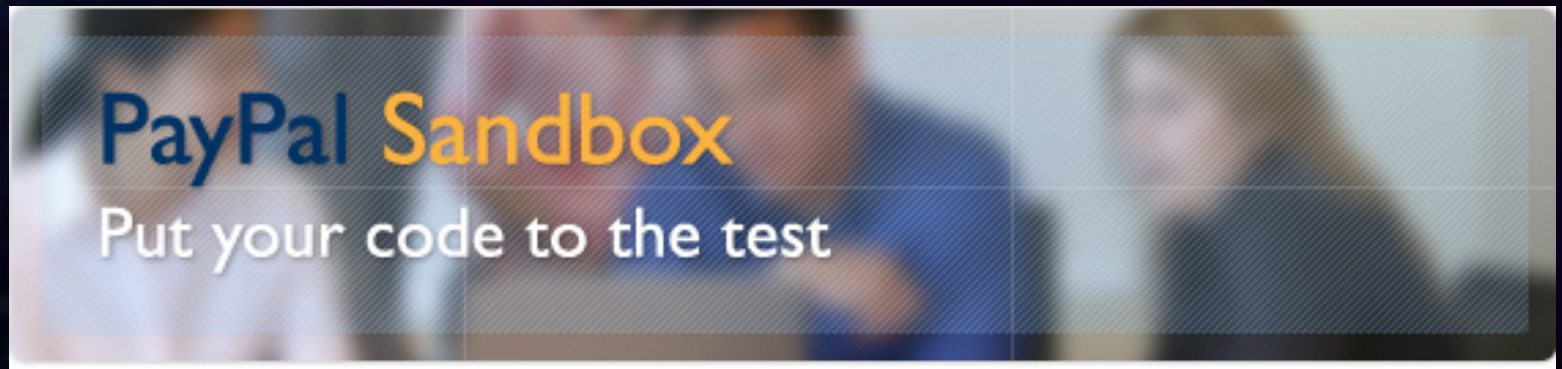
MERCHANT ACCOUNT

Popular Merchant Service Providers

- PayPal (Verisign Payflow Pro)
- CyberSouce (Authorize.net)
- First Data (LinkPoint International)

Setting up PayPal





The PayPal Sandbox allows you to test the integration of your PayPal payment solution before submitting transactions to the live PayPal environment. The Sandbox is a duplicate of the live PayPal site, except that no real money changes hands.

Test Accounts

Create a preconfigured buyer or seller account.

Create a Website Payments Pro account (new release).

Manually create accounts.

Test Email

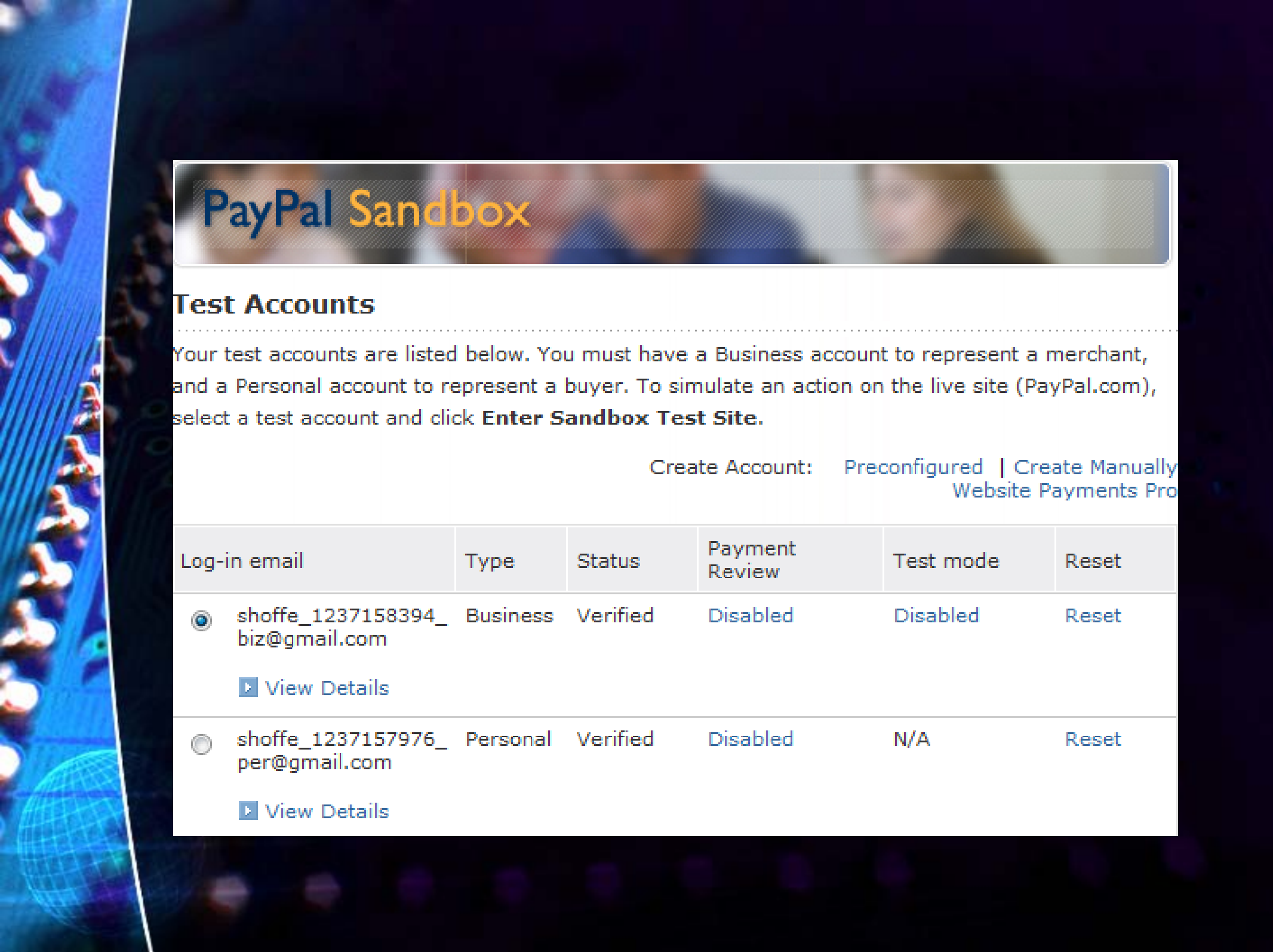
Access email sent to your test accounts.

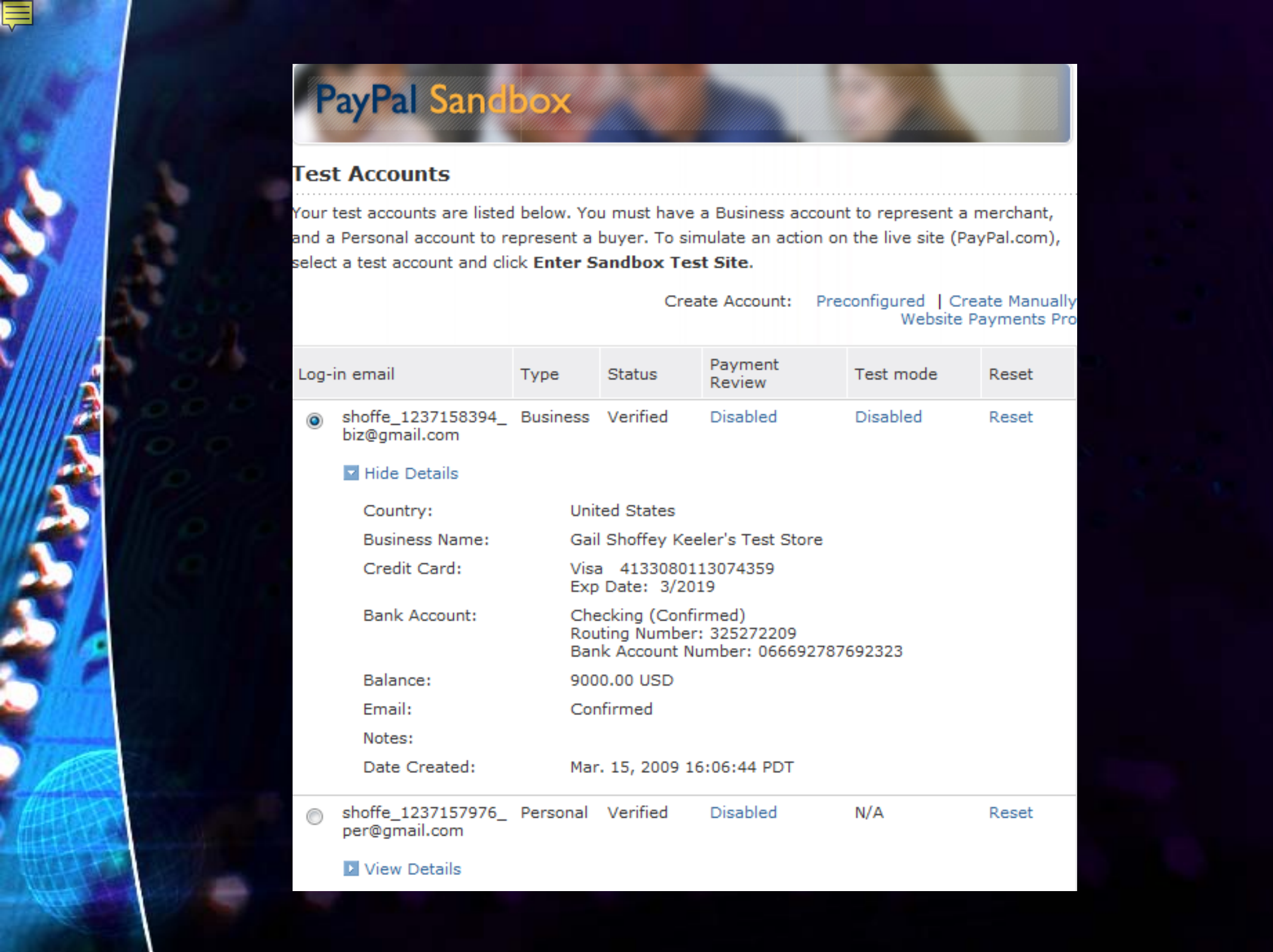
API Credentials

Manage API credentials for your test accounts.

Test Tools

Instant Payment Notification (IPN) simulator


PayPal Sandbox
Test Accounts
Your test accounts are listed below. You must have a Business account to represent a merchant, and a Personal account to represent a buyer. To simulate an action on the live site (PayPal.com), select a test account and click Enter Sandbox Test Site.
Create Account: Preconfigured | Create Manually
Website Payments Pro
Log-in email
Type
Status
Payment Review
Test mode
Reset
shoffe_1237158394_biz@gmail.com
Business
Verified
Disabled
Disabled
Reset
View Details
shoffe_1237157976_per@gmail.com
Personal
Verified
Disabled
N/A
Reset
View Details


PayPal Sandbox
Test Accounts
Your test accounts are listed below. You must have a Business account to represent a merchant, and a Personal account to represent a buyer. To simulate an action on the live site (PayPal.com), select a test account and click Enter Sandbox Test Site.
Create Account: Preconfigured | Create Manually
Website Payments Pro
Log-in email
Type
Status
Payment Review
Test mode
Reset
shoffe_1237158394_biz@gmail.com
Business
Verified
Disabled
Disabled
Reset
Hide Details
Country: United States
Business Name: Gail Shoffey Keeler's Test Store
Credit Card: Visa 4133080113074359
Exp Date: 3/2019
Bank Account: Checking (Confirmed)
Routing Number: 325272209
Bank Account Number: 066692787692323
Balance: 9000.00 USD
Email: Confirmed
Notes:
Date Created: Mar. 15, 2009 16:06:44 PDT
shoffe_1237157976_per@gmail.com
Personal
Verified
Disabled
N/A
Reset
View Details

PayPal Sandbox

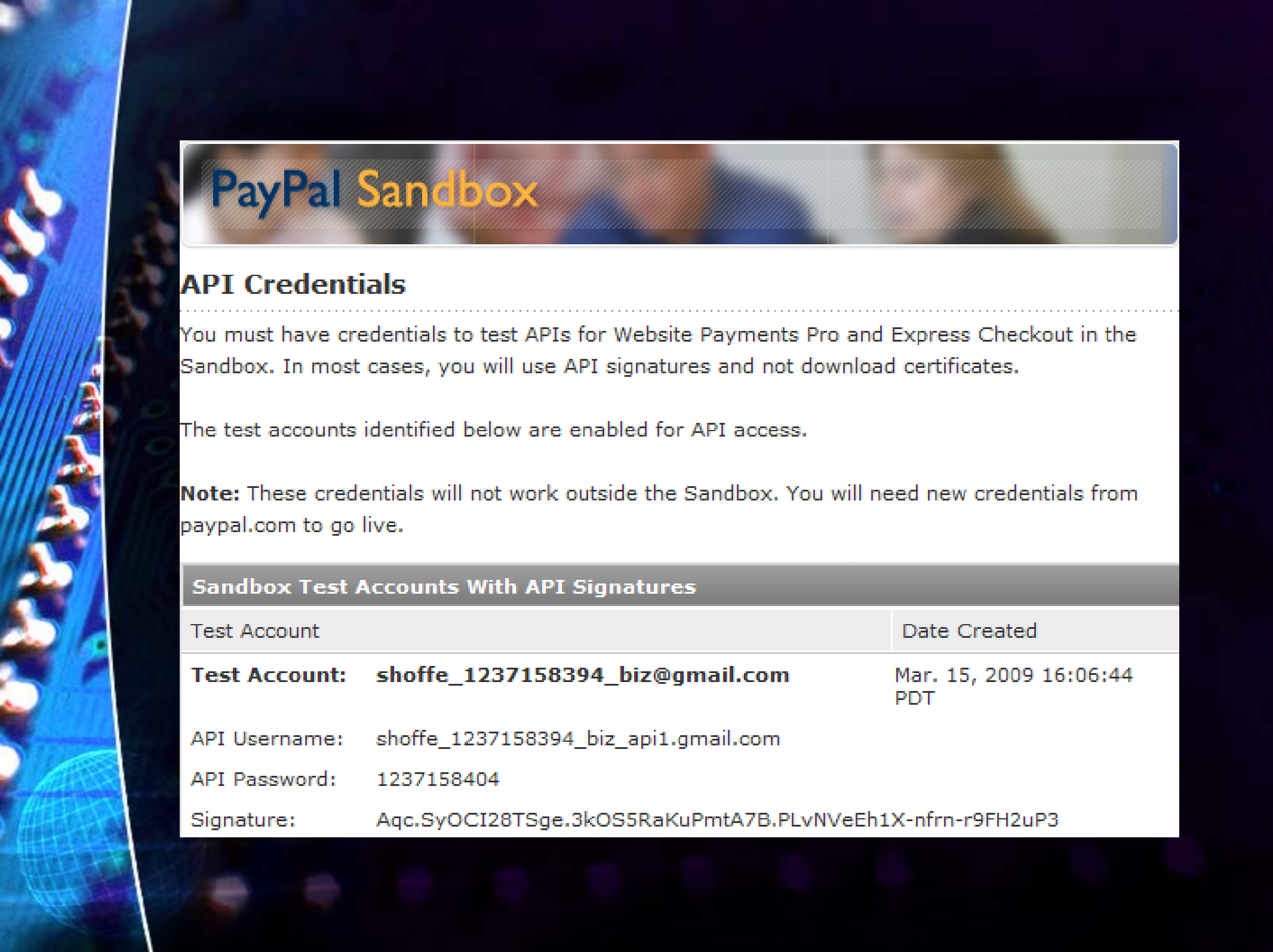
Test Email

Test account email addresses are not real. Email sent to them is never delivered outside the Sandbox.

Below are the most recent messages sent to your Sandbox test accounts.

Inbox

To	From	Subject	Date
shoffe_1237158394_biz@gmail.com	service@paypal.com	Your application has been approved	Mar. 15, 2009 16:06:43 PDT
shoffe_1237158200_per@gmail.com	service@paypal.com	You have successfully lifted your PayPal withdrawal limit	Mar. 15, 2009 16:03:24 PDT
shoffe_1237158087_biz@gmail.com	service@paypal.com	Your application has been approved	Mar. 15, 2009 16:01:32 PDT
shoffe_1237157976_per@gmail.com	service@paypal.com	You have successfully lifted your PayPal withdrawal limit	Mar. 15, 2009 15:59:39 PDT


PayPal Sandbox
API Credentials
You must have credentials to test APIs for Website Payments Pro and Express Checkout in the Sandbox. In most cases, you will use API signatures and not download certificates.
The test accounts identified below are enabled for API access.
Note: These credentials will not work outside the Sandbox. You will need new credentials from paypal.com to go live.
Sandbox Test Accounts With API Signatures
Test Account
Date Created
Test Account: shoffe_1237158394_biz@gmail.com
Mar. 15, 2009 16:06:44 PDT
API Username: shoffe_1237158394_biz_api1.gmail.com
API Password: 1237158404
Signature: Aqc.SyOCI28TSge.3kOS5RaKuPmtA7B.PLvNVeEh1X-nfrn-r9FH2uP3

My Account Overview

Welcome, **Gail Shoffey Keeler** (shoffe_1237158394_biz@gmail.com) Edit profile
Business Name: Gail Shoffey Keeler's Test Store
Account holder since 2009
Account type: Business
Status: Verified (New)

PayPal balance

Currency	Available	Pending	Balance
U.S. Dollar:	$9,000.00 USD	$1,510.49 USD	$10,510.49 USD

To do list (2)

- Accept payment - Someone sent you money - find out how to accept it
- Add Phone - We may contact you if we notice unusual account activity

See all steps

1 Sign up for a Business Account. — Complete

2 Verify your information — Complete

3 Set up your payment solution

Step	Info Required	Time to Complete	Action
Virtual Terminal			
Submit application			Approved
Complete Billing Agreement (BA) (required)		2 minutes	Go
Apply for Virtual Terminal			

Get Started | Virtual Terminal Manual (PDF)

See all steps

Account history: All account activity | Payments sent | Payments received

Recent activity - Last updated 4/14/2009 19:54 PDT

File	Type	To/From	Name/Email/Phone	Date	Status	Details	Action	Amount ($)	Fee
☐	Payment Received	From	Test User	Apr. 14, 2009	Under Review	Details		$1,555.91 USD	-$45.42 USD

File Selected Items | File All

My Account Overview

Welcome, **Gail Shoffey Keeler** (shoffe_1237158394_biz@gmail.com) Edit profile
Business Name: Gail Shoffey Keeler's Test Store
Account holder since 2009
Account type: Business
Status: Verified (New)

PayPal balance			
Currency	Available	Pending	Balance
U.S. Dollar:	$9,000.00 USD	$1,510.49 USD	$10,510.49 USD

To do list (2)

- Accept payment - Someone sent you money - find out how to accept it
- Add Phone - We may contact you if we notice unusual account activity

See all steps

1 Sign up for a Business Account. — Complete

2 Verify your information — Complete

3 Set up your payment solution

Step	Info Required	Time to Complete	Action
Virtual Terminal			
Submit application			Approved
Complete Billing Agreement (BA)			Complete
Apply for Virtual Terminal			Go

Get Started | Virtual Terminal Manual (PDF)

See all steps

Account history: All account activity | Payments sent | Payments received

Recent activity - Last updated 4/14/2009 19:55 PDT

File	Type	To/From	Name/Email/Phone	Date	Status	Details	Action	Amount ($)	Fee
☐	Payment Received	From	Test User	Apr. 14, 2009	Under Review	Details		$1,555.91 USD	-$45.42 USD

File Selected Items | File All

Virtual Terminal - Enter Transaction

Secure Transaction

* Required Hide optional fields

Details

*Currency: U.S. Dollars

*Net Order Amount: $

Shipping: $ Apply tax to shipping

Tax Rate: 0.000 %

Tax Amount: $ 0.00

Total: $ 0.00

*Transaction Type: Sale

Item Name/Service:

Order Number:

Comment:

Billing Information - Please enter the following information exactly as it appears on the customer's credit card statement.

Country: United States

First Name:

Last Name:

*Card Type:

*Card Number:

*Expiration Date: 01 2009

Card Security Code: (On the back of your card, locate the final 3 digit number)
What's this? Using Amex?

Address Line 1:

Address Line 2:

City:

State:

ZIP Code:

Email Address:

Home Telephone:

Shipping Address

- No shipping address required
- Use the same above billing address as the shipping address
- Enter a separate shipping address

Review Transaction | Cancel

Security

PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD (DSS) COMPLIANCE

Overview

- About PCI compliance
- PCI DSS history
- Introduction to compliance
- The 12 requirements
- The 6 steps towards compliance
- What to prepare for PCI validation compliance

About PCI Compliance

- Requires compliance if you store, process, transmit or handle cardholder data
  - Current version is 1.2 (Oct. 2008)
- Secure your business
  - Intellectual and Web property
- Better application design
  - Emphasis on security
- Peace of mind for customers

PCI History

- 5 major credit card brands:
  - Visa Inc.
  - MasterCard Worldwide
  - American Express
  - Discover Financial Services
  - JCB International
- PCI Security Council founded in June 2005
  - Concern about competitor brand-specific requirements intersecting
  - Collaborated to for a single standard for protecting credit card data
- Based on ISO 17799 – Information technology - Security techniques - Code of practice for information security management
  - Defined 12 main requirements

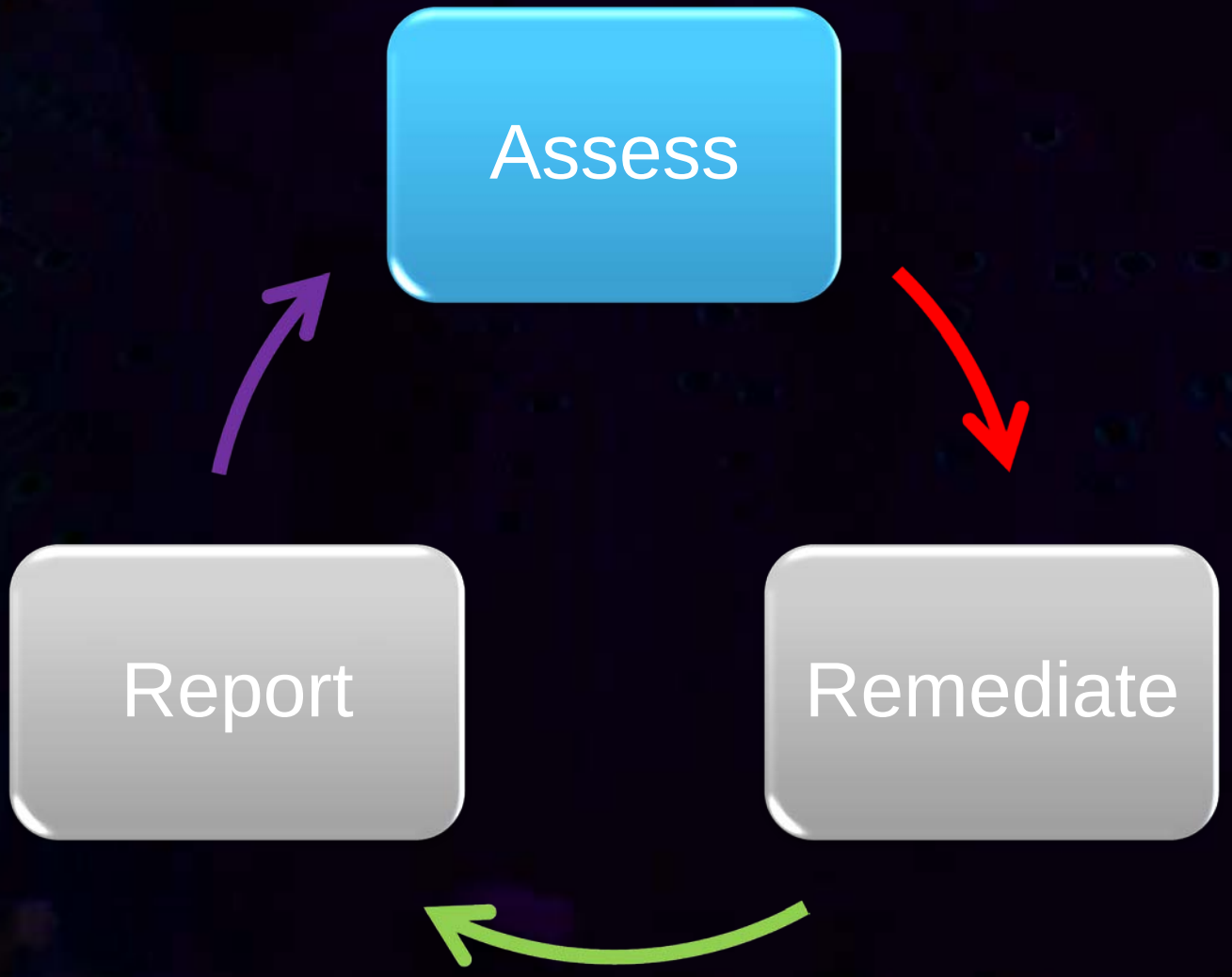
Introduction

- According to Privacy Rights Clearinghouse.org, more than 234 million records with sensitive information have been breached since January 2005
- A survey of businesses in the U.S. and Europe reveals activities that may put cardholder data at risk:

Source: Forrester Consulting: The State of PCI Compliance (commissioned by the RSA/EMC)

- 81% store payment card number
- 73% store payment card expiration dates
- 71% store payment card verification codes
- 57% store customer data from the payment card magnetic stripe
- 16% store other personal data

PCI Compliance Process



12 Requirements and Security Assessment Procedures V 1.2

Build and Maintain a Secure Network

1. Install and maintain a PCI-compliant firewall
2. Do not use default system or application passwords

Protect Cardholder Data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications

12 Requirements and Security Assessment Procedures V 1.2

Implement Strong Access Control Measures

7. Restrict access to cardholder data
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security for employees and contractors

Compensating Controls for PCI

If you cannot meet a requirement then you must have a legitimate business reason *and* it must be reviewed by a Qualified Security Assessor (QSA)

6 Step Approach to Compliance

1. Remove sensitive authentication data and limit data retention
   - If you don’t need it, don’t store it
2. Protect the perimeter, internal, and wireless networks
   - Points of access to most compromises
3. Secure payment card applications
   - Processes and servers

6 Step Approach to Compliance

4. Monitor and control access to your system
   - Who, what, when, and how is the data being accessed
5. Protect stored cardholder data
   - Use key protection mechanisms
6. Finalize remaining compliance ensuring all controls are in place
   - Remaining policies, procedures, and processes

Prepare for an Assessment

- Gather documentation
- Schedule Resources
- Describe the Environment

Application Programming Interface

CODING TO AN API

Types of Connections

- Virtual Terminal
- Hosted Order Page
- Silent Order Post
- API – Payment Gateway

Application Programming Interface

- The Application Programming Interface (API) consists of several sets of related methods or functions that specifies how two different computers can communicate
- Platform independent

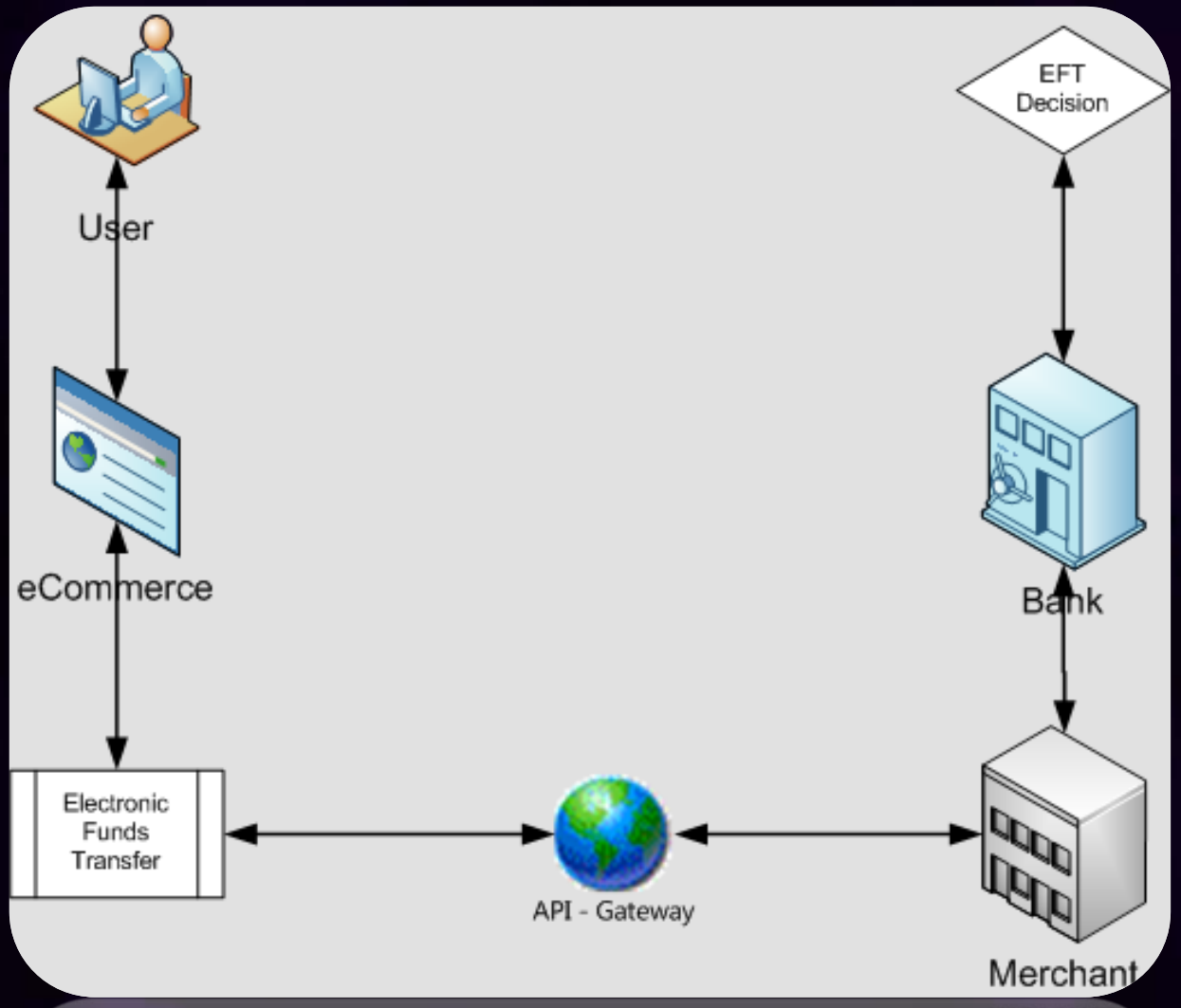
Why API is Preferred

- Keeps the customer on your website
- Customer order tracking – line items, tax
- Greater stability than with a web browser
- Scalable for large volume processing
- Security control

EFT Flow

Electronic Funds Transfer (EFT)

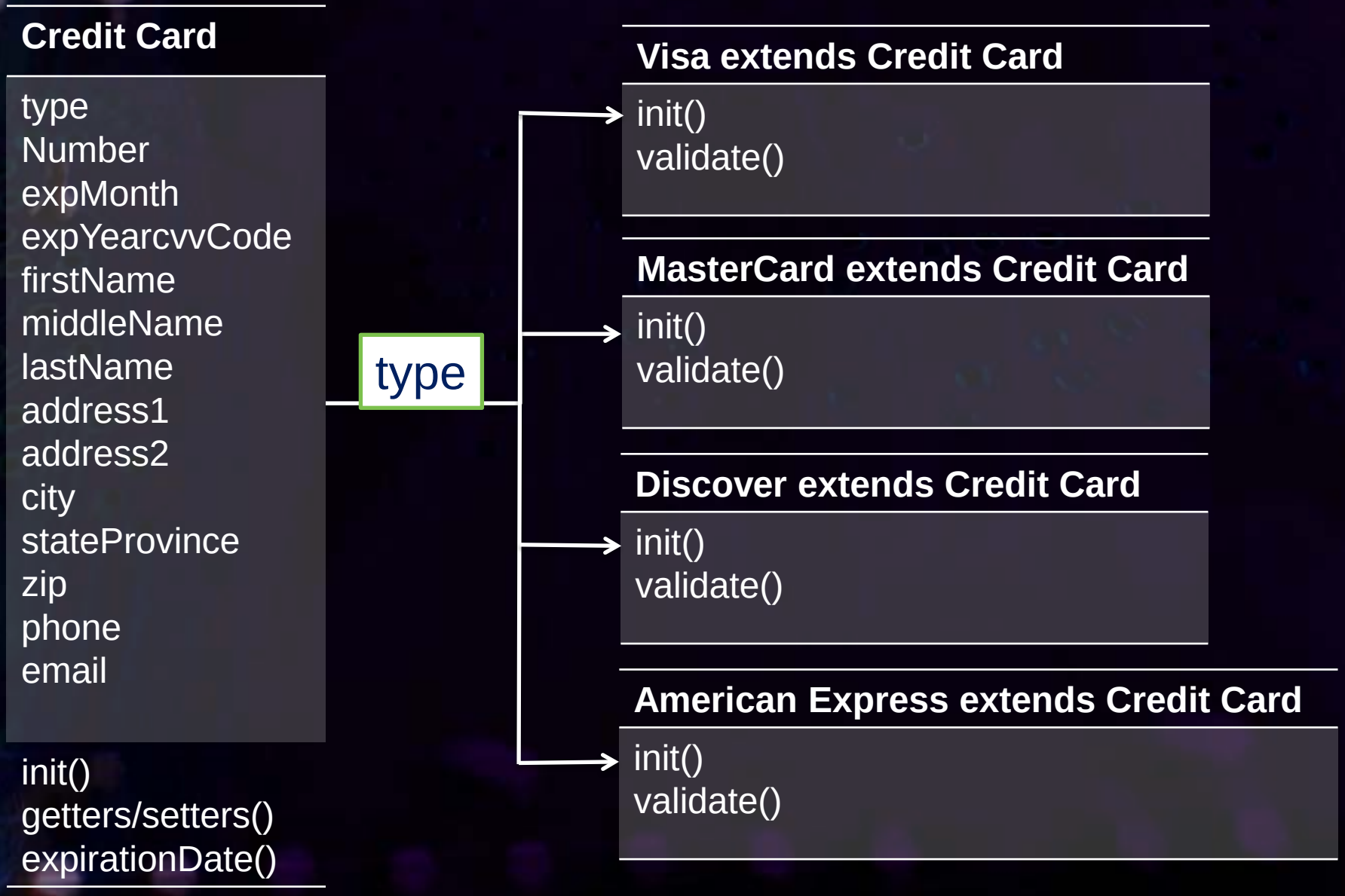
1. Order Placed
2. Authorization Request
3. Authorization Response
4. Order Fulfilled
5. Settlement Request
6. Settlement Deposited



Ex: General Processing

- Load configuration files
- Parse the properties
- Add merchant specific values
- Create a properties object
- Create a credit card object
- Combine the objects into one transaction
- Process the response

Ex: Credit Card Components



Summary

- Payment processing offers the user an uncomplicated and seamless purchasing experience
- Your organization will:
  - Increase workplace efficiency and security while reducing errors
  - Get paid in real time which will improve the cash flow to vendors
- A PCI Compliant environment:
  - Secures your business
  - Promotes better application design
- Peace of mind for customers

Tools for Assessing Security

- Although the counsel sets the standards, each card brand has its own program for assessing compliance, validation levels, and enforcement
  - Visa Inc: www.visa.com/cisp
  - Visa Europe: http://www.visaeurope.com/aboutvisa/security/ais/aisprogramme.jsp
  - MasterCard Worldwide: www.mastercard.com/sdp
  - American Express: www.americanexpress.com/datasecurity
  - Discover Financial Services: http://www.discovernetwork.com/fraudsecurity/disc.html
  - JCB International: www.jcb-global.com/english/pci/index.html

CF Code Examples

- PayPal has made it extremely easy:
  - Download: https://cms.paypal.com/us/cgi-bin/?cmd=_render-content&content_ID=developer/library_download_sdks
- Easy CFM:
  - http://www.easycfm.com/coldfusion/tutorials/index.cfm?categoryid=4
    - Shopping carts
    - Authorize.net

References

- Bragg, M. (n. d). Payment processing basics. Retrieved April 2, 2009, from http://www2.eventsvc.com/paypaldev/payment_od
- Merchant Equipment Store. (2009). *Online and Internet merchant accounts*. Retrieved April 5, 2009, from http://www.merchantequip.com/merchant-accounts/credit-card-processing/e-commerce-internet/
- PCI Quick Reference Guide. (n. d.). *Understanding the payment card industry data security standard version 1.2*. Retrieve April 3, 2009, from PCI Security Council Website: https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf
- PCI Security Standards Council. (2008, October). *Payment Card Industry (PCI) Data Security Standard Version 1.2*. Retrieved April 1, 2009, from PCI Security Standards Council Website: https://www.pcisecuritystandards.org/security_standards/pci_dss_download.html
- PCI Security Standards Council. (2009 March 31). *Prioritized approach for DSS 1.2*. Retrieved April 1, 2009, from PCI Security Standards Council Website: https://www.pcisecuritystandards.org/education/prioritized.shtml

Your Questions & Comments

Gail “Montreal” Shoffey Keeler
shoffey@gmail.com
Twitter: shoffey
LinkedIn: (Gail Shoffey Keeler)
Facebook: (Gail Shoffey)