Certificate & Key Management Requirements for WebCrypto

Vijay Bharadwaj & Israel Hilerio

User Requirements*

- Users need to be able to manage their certificates and keys independent of transactions
  - Not all certificates and keys are associated with a domain of origin (e.g. hardware bound certificates and keys)
  - Some 3rd party certificates or keys, could be managed outside the browser
- User need to be able to select which certificates or keys they want to use to complete a transaction
  - That implies that a list of all available certificates or keys needs to be available to end-users
  - Not all certificates or keys are valid for all transactions
    - The mapping between certificates or keys and allowed transactions is defined by the server
- Users need to be able to generate new certificates or keys as part of their workflow if they don't happen to own a certificate or key that matches a specific transactions
  - That implies the ability to generate a certificate or a key from a browser session
- Certificates and keys can be stored locally on the machine or in a portable device
  - Smart Cards, Machine Certificate Stores, Secured USB Keys, etc.

* This Proposal doesn't deal with how to write certificates or keys back to external devices or outside the browser storage technologies. That is out of scope for this proposal.

Certificate & Key Management Requirements:
Existing Capabilities

Existing Web APIs or Polyfills

- Provision Certificate
  - Combining the usage of existing APIs can support this action: XHR, IDB, WebCrypto
  - Can be delivered to developers as a polyfill
- Processing operations
  - Handle Response – no different that what can be returned by an XHR request today (blob, ArrayBuffer, JSON)
  - Generate/Send confirmation – supported by web polyfills
  - Solve Crypto Challenge – Enabled by WebCrypto
- Storage operations
  - Create, read, and delete certificates can be done using existing browser technologies
  - Create, read, and delete keys can be done using existing browser technologies

Server Side

- Required certificate operations:
  - Update
  - Revoke
  - Validate timeline

Certificate & Key Management Requirements:

New Requirements

- New operations
  - Generate Key
  - GetKey
  - Sign w/Key
  - GetCertificate
- Access to certificates and keys on external devices
  - Certificates and Keys need to be able to be stored and retrieved seamlessly without the developer having to know the device in which they are persisted

In Summary

- GenerateCertifcateRequest, GenerateCertificationConfirmation, HandleResponse
  - We are expecting the issuer to provide a series of polyfills that will ensure the correct handshake to the server
  - Most of these operations will leverage XHR behind the scenes
- Using 3rd Party Keys and Certificates with websites
  - During the provisioning process, iframes can be used to exchange provisioned certificates between issuers and consumers
- The only thing requires browser support
  - Provide the basic crypto and network operations
  - Provide a mechanism for the user to view and select certifications and keys
  - Provide a mechanism via domain based stores (IDB, WebStorage, FileAPIs, etc.) to save certificates and keys
    - This implies that access to this information will be enabled by having iframes that provide access to the host via postMessage
  - Provide a user interface to manage your keys (outside of the scope of the JS APIs)

Scenario Flows

1. Using pre-provisioned key from external device
2. Acquiring new key from the web

Using pre-provisioned key from external device

Payment Scenario

Bank1

Welcome, Pedro My Settings | Security | Secure Message(s) | ATMs/Branches | Help | **Logout**

Search or ask a question

MY ACCOUNTS | CHECKING & SAVINGS | LOANS & CREDIT | ONLINE SERVICES | INVESTMENTS | INSURANCE

Thursday, October 23, 2014 11:57 AM (Pacific) Printer Friendly

Quick Links

- Balances
- Statements
- Transfer/Payment
- e-Alerts
- Withdraw
- Pay Bills
- Stop Payment
- Logout

Open New Account

Select...

BillPay

Pop Up Blocker?

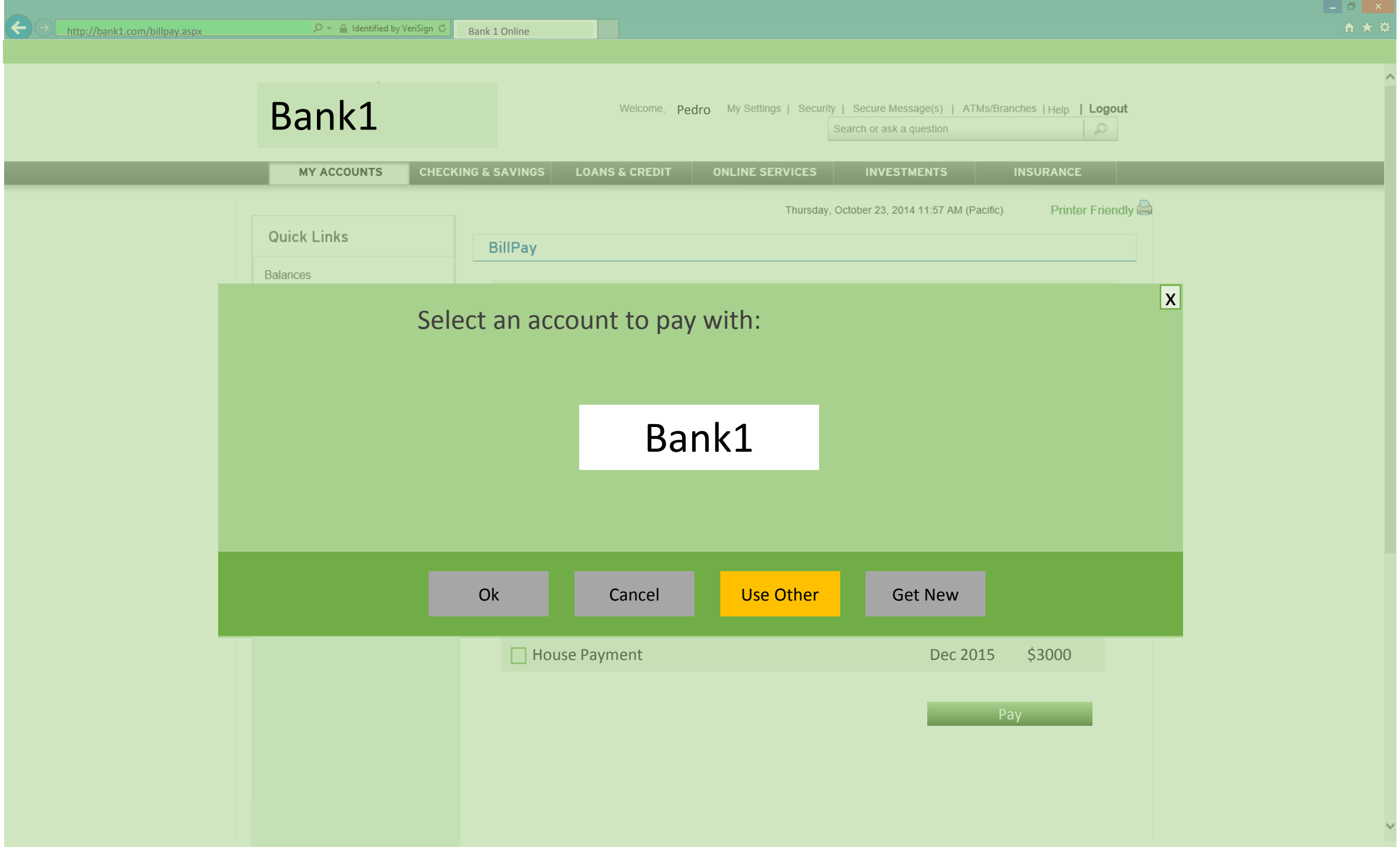
The BillPay window should appear automatically. If you have a pop-up blocker installed, please click the button below.

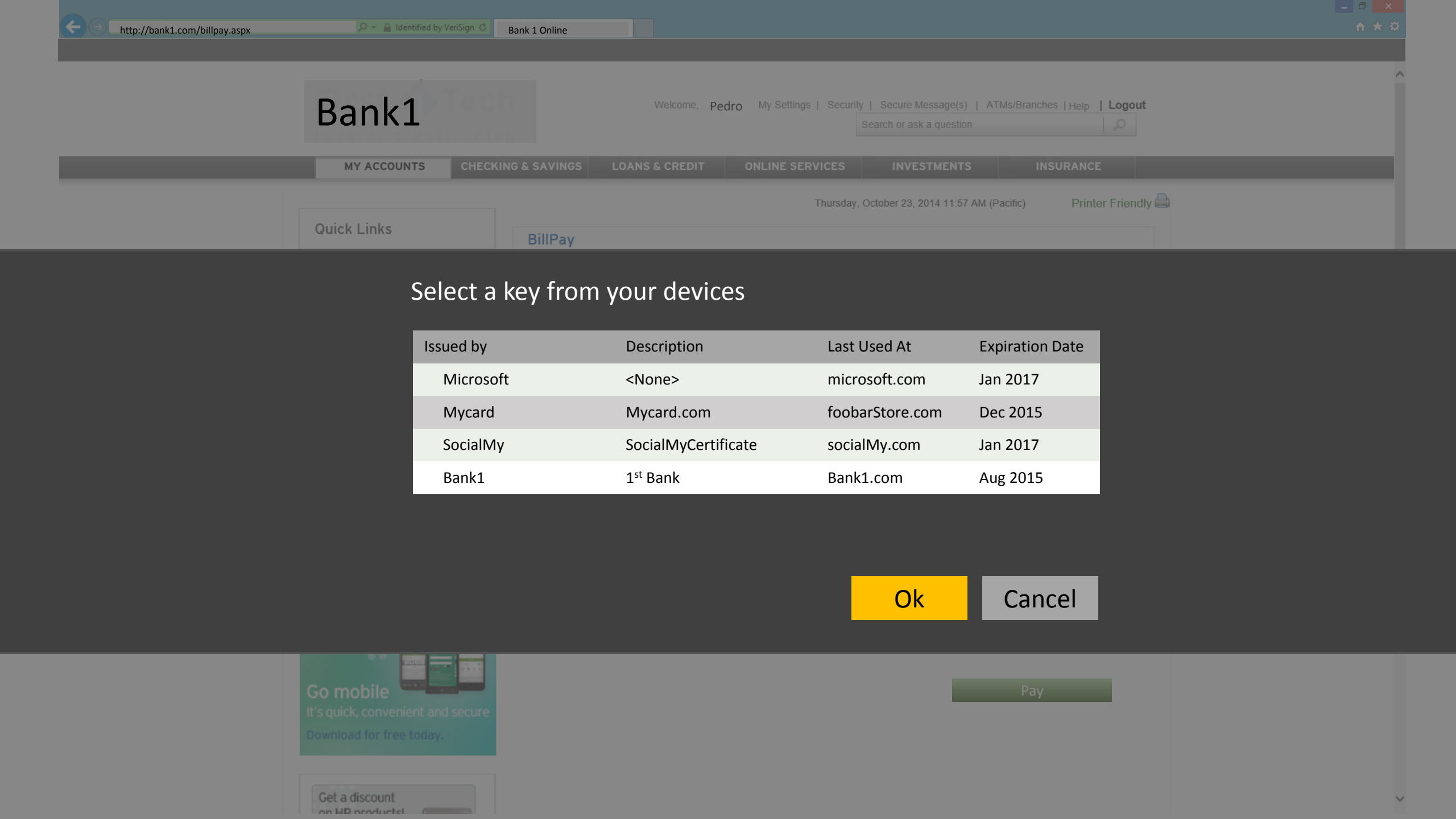
GO TO BILLPAY

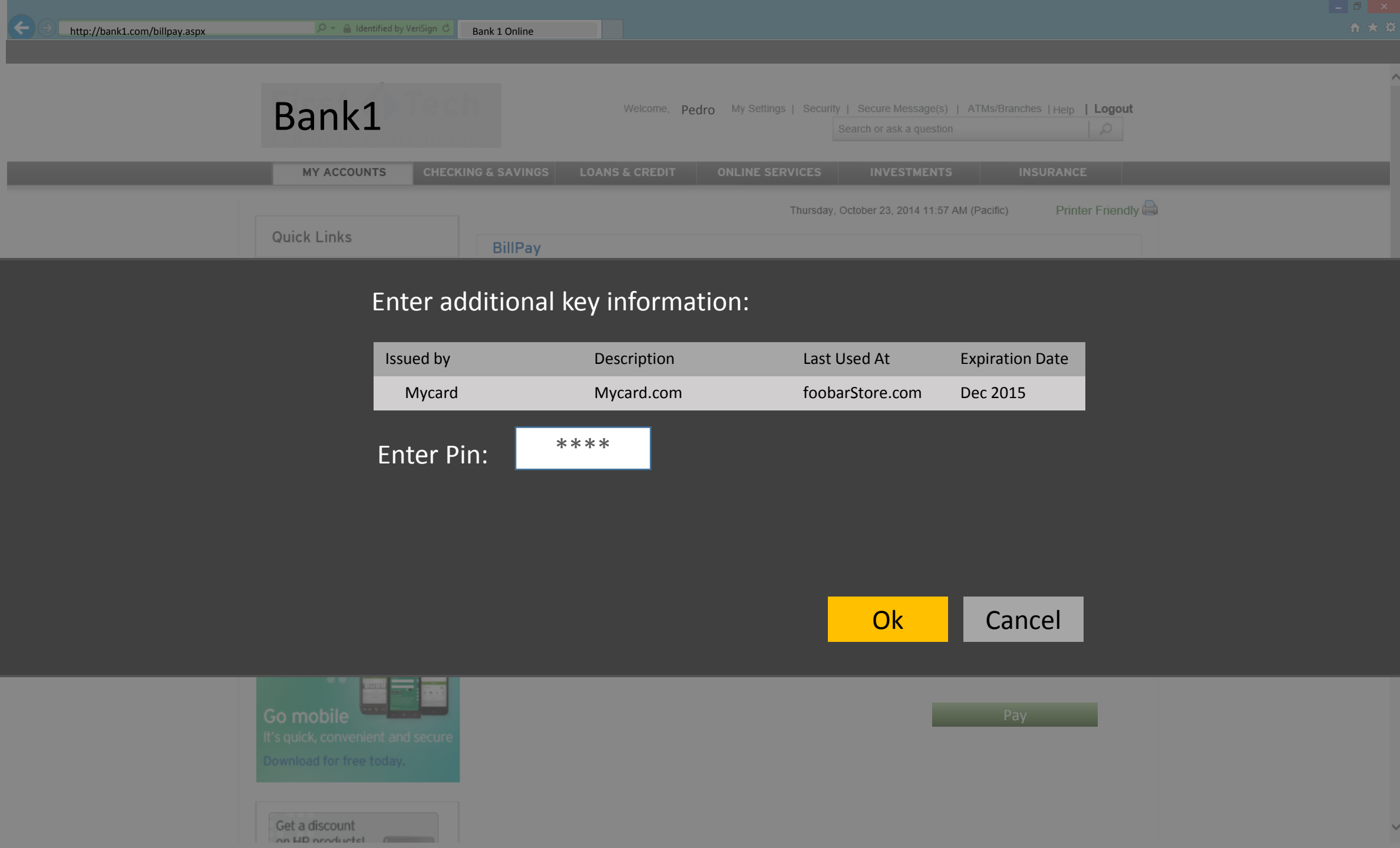
Pay Bills

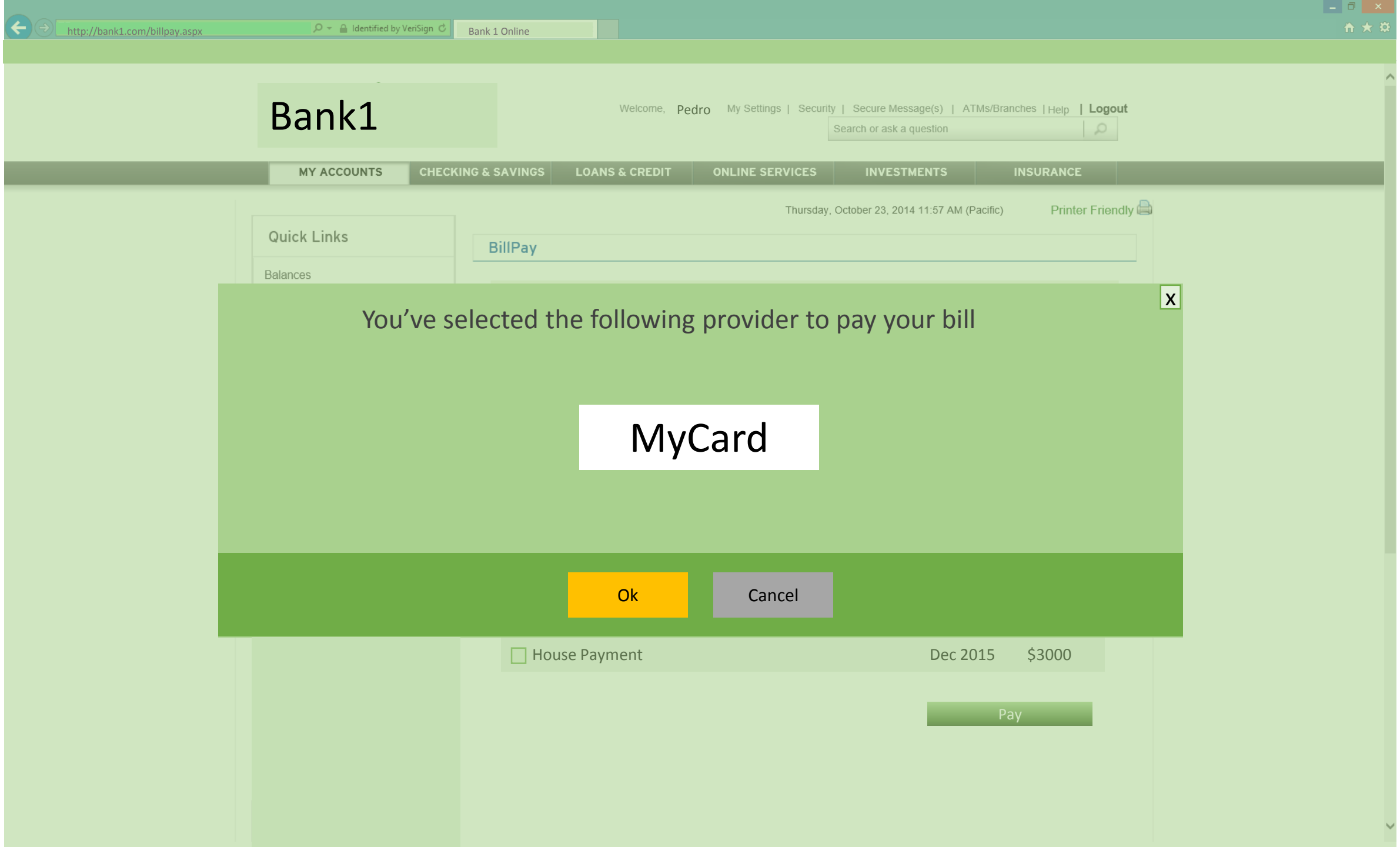
Payee	Due Date	Amount
[x] School Tuition	Nov 2015	$100
[ ] Visa	Dec 2015	$1000
[ ] Puget Sound Electricity	Dec 2015	$500
[ ] Car Payment	Dec 2015	$150
[ ] House Payment	Dec 2015	$3000

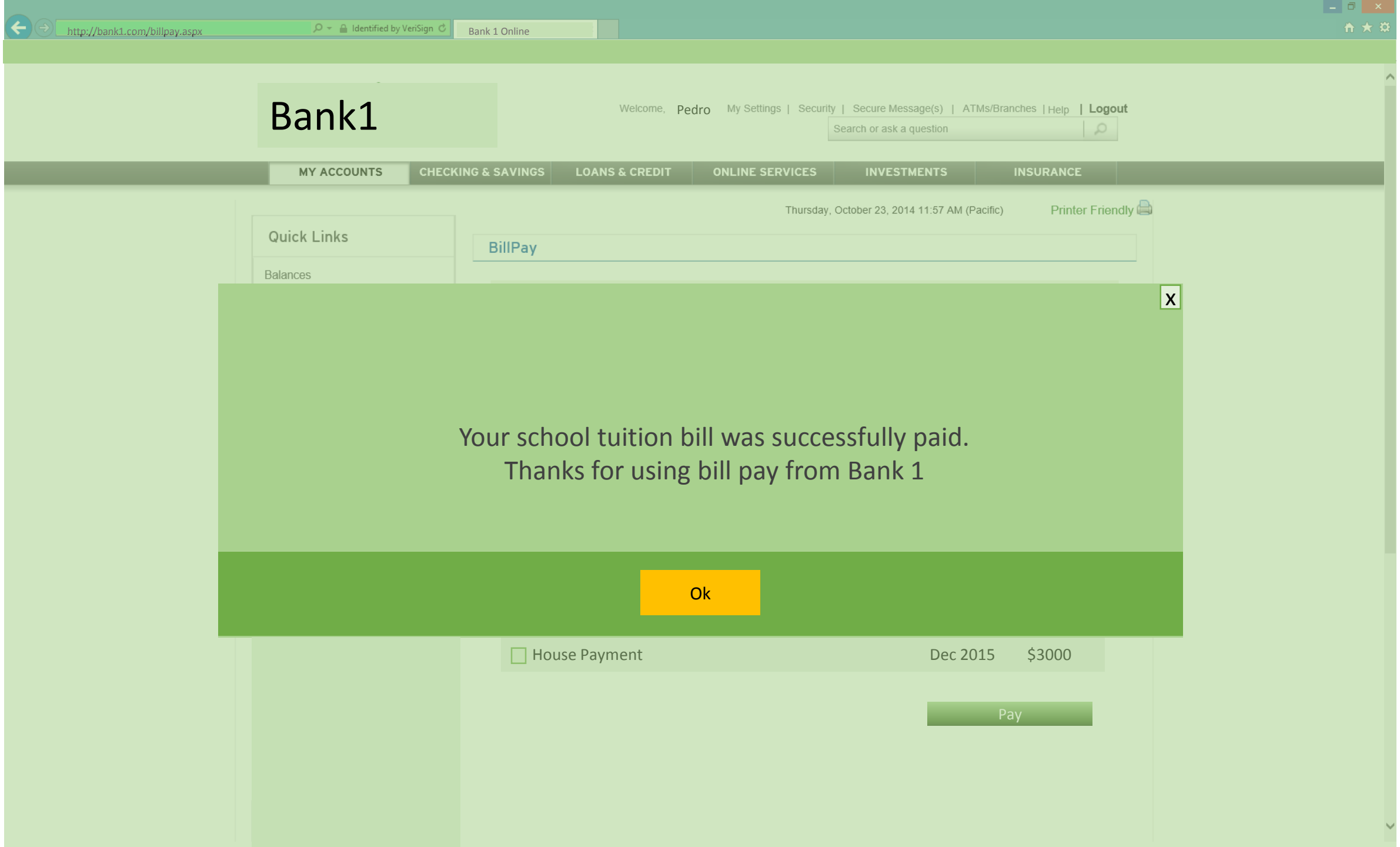
Pay


http://bank1.com/billpay.aspx
Identified by VeriSign
Bank 1 Online
Bank1
Welcome, Pedro
My Settings | Security | Secure Message(s) | ATMs/Branches | Help | Logout
Search or ask a question
MY ACCOUNTS
CHECKING & SAVINGS
LOANS & CREDIT
ONLINE SERVICES
INVESTMENTS
INSURANCE
Thursday, October 23, 2014 11:57 AM (Pacific)
Printer Friendly
Quick Links
Balances
BillPay
X
Select an account to pay with:
Bank1
Ok
Cancel
Use Other
Get New
House Payment
Dec 2015
$3000
Pay


http://bank1.com/billpay.aspx
Identified by VeriSign
Bank 1 Online
Bank1
Welcome, Pedro
My Settings | Security | Secure Message(s) | ATMs/Branches | Help | Logout
Search or ask a question
MY ACCOUNTS
CHECKING & SAVINGS
LOANS & CREDIT
ONLINE SERVICES
INVESTMENTS
INSURANCE
Thursday, October 23, 2014 11:57 AM (Pacific)
Printer Friendly
Quick Links
BillPay
Select a key from your devices
Issued by
Description
Last Used At
Expiration Date
Microsoft
<None>
microsoft.com
Jan 2017
Mycard
Mycard.com
foobarStore.com
Dec 2015
SocialMy
SocialMyCertificate
socialMy.com
Jan 2017
Bank1
1st Bank
Bank1.com
Aug 2015
Ok
Cancel
Go mobile
It's quick, convenient and secure
Download for free today.
Pay
Get a discount

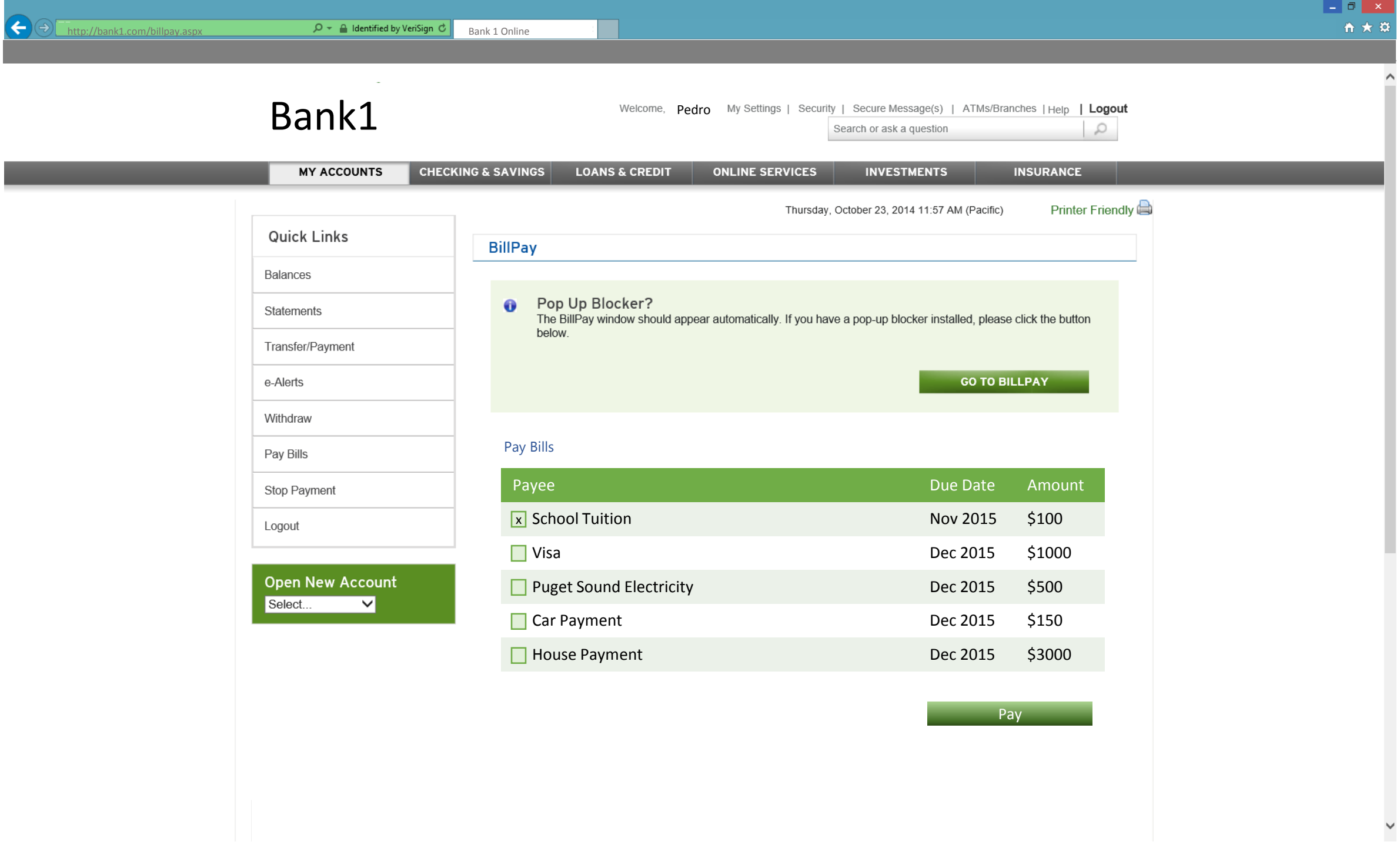

http://bank1.com/billpay.aspx
Identified by VeriSign
Bank 1 Online
Bank1
Welcome, Pedro
My Settings | Security | Secure Message(s) | ATMs/Branches | Help | Logout
Search or ask a question
MY ACCOUNTS
CHECKING & SAVINGS
LOANS & CREDIT
ONLINE SERVICES
INVESTMENTS
INSURANCE
Thursday, October 23, 2014 11:57 AM (Pacific)
Printer Friendly
Quick Links
BillPay
Enter additional key information:
Issued by
Description
Last Used At
Expiration Date
Mycard
Mycard.com
foobarStore.com
Dec 2015
Enter Pin:
****
Ok
Cancel
Go mobile
It's quick, convenient and secure
Download for free today.
Pay
Get a discount

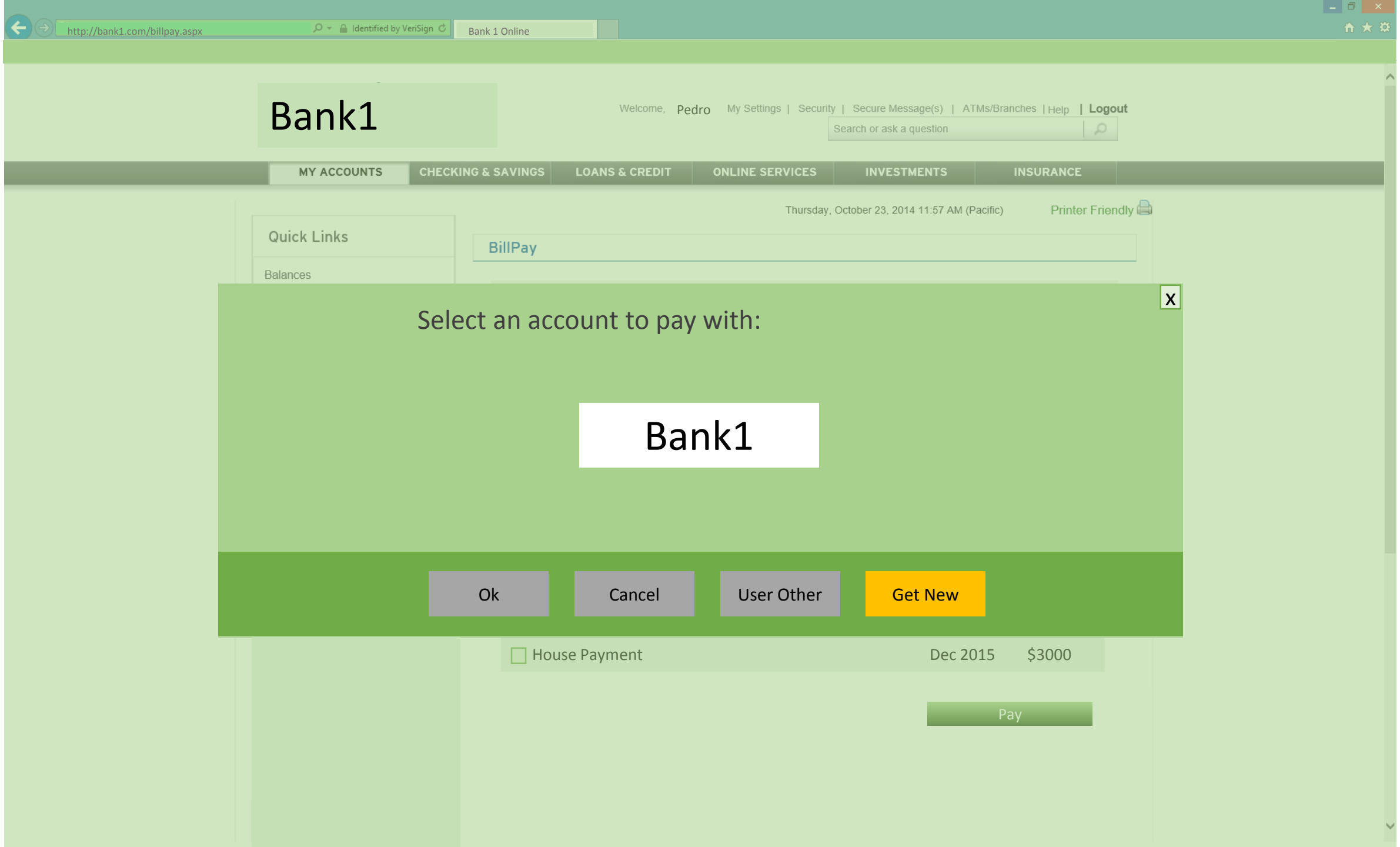

http://bank1.com/billpay.aspx
Identified by VeriSign
Bank 1 Online
Bank1
Welcome, Pedro
My Settings | Security | Secure Message(s) | ATMs/Branches | Help | Logout
Search or ask a question
MY ACCOUNTS
CHECKING & SAVINGS
LOANS & CREDIT
ONLINE SERVICES
INVESTMENTS
INSURANCE
Thursday, October 23, 2014 11:57 AM (Pacific)
Printer Friendly
Quick Links
Balances
BillPay
X
You've selected the following provider to pay your bill
MyCard
Ok
Cancel
House Payment
Dec 2015
$3000
Pay

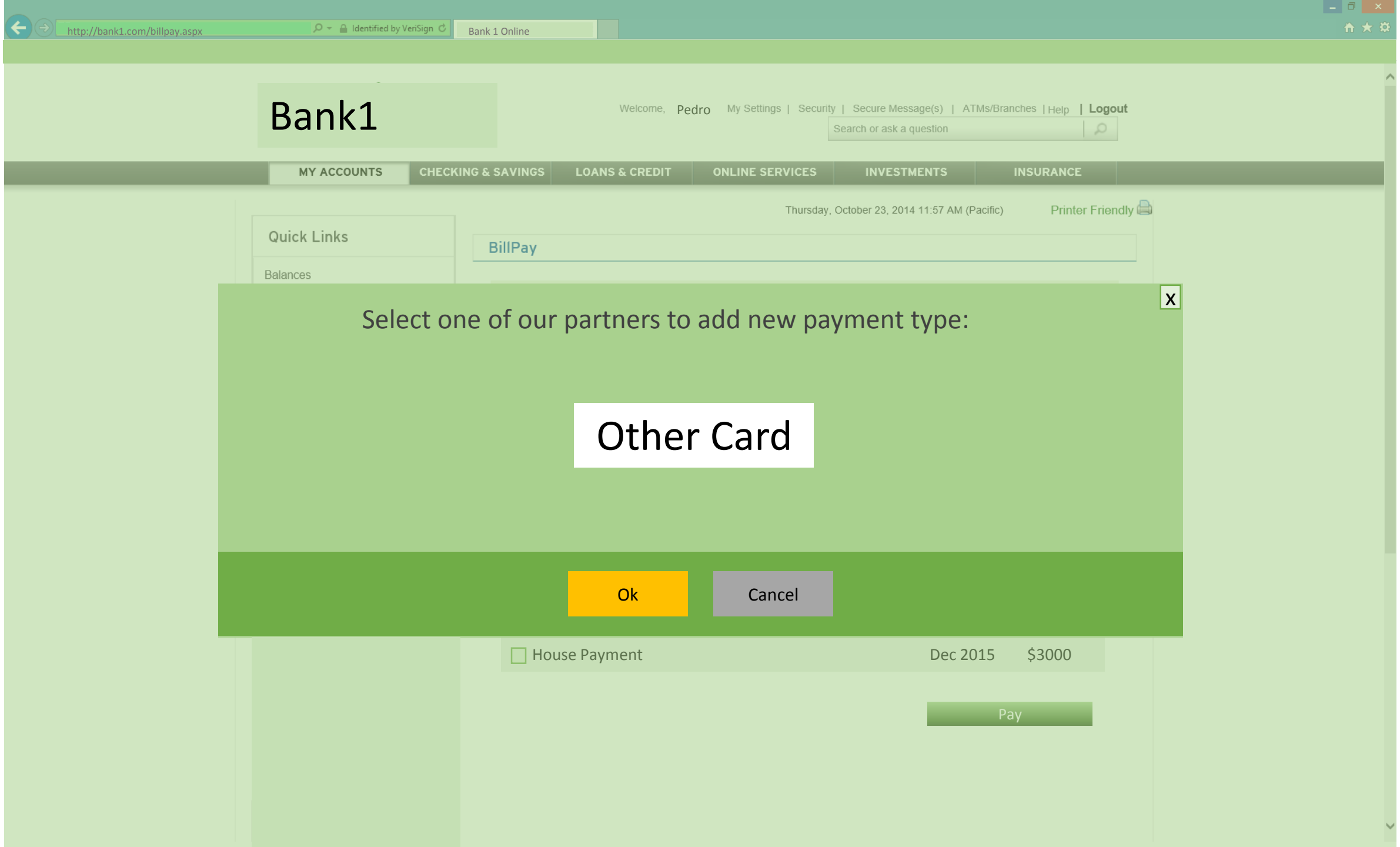

http://bank1.com/billpay.aspx
Identified by VeriSign
Bank 1 Online
Bank1
Welcome, Pedro
My Settings | Security | Secure Message(s) | ATMs/Branches | Help | Logout
Search or ask a question
MY ACCOUNTS
CHECKING & SAVINGS
LOANS & CREDIT
ONLINE SERVICES
INVESTMENTS
INSURANCE
Thursday, October 23, 2014 11:57 AM (Pacific)
Printer Friendly
Quick Links
Balances
BillPay
X
Your school tuition bill was successfully paid.
Thanks for using bill pay from Bank 1
Ok
House Payment
Dec 2015
$3000
Pay

Acquiring new key from the web

Payment Scenario


http://bank1.com/billpay.aspx
Identified by VeriSign
Bank 1 Online
Bank1
Welcome, Pedro
My Settings | Security | Secure Message(s) | ATMs/Branches | Help | Logout
Search or ask a question
MY ACCOUNTS
CHECKING & SAVINGS
LOANS & CREDIT
ONLINE SERVICES
INVESTMENTS
INSURANCE
Thursday, October 23, 2014 11:57 AM (Pacific)
Printer Friendly
Quick Links
Balances
Statements
Transfer/Payment
e-Alerts
Withdraw
Pay Bills
Stop Payment
Logout
Open New Account
Select...
BillPay
Pop Up Blocker?
The BillPay window should appear automatically. If you have a pop-up blocker installed, please click the button below.
GO TO BILLPAY
Pay Bills
Payee
Due Date
Amount
x School Tuition
Nov 2015
$100
Visa
Dec 2015
$1000
Puget Sound Electricity
Dec 2015
$500
Car Payment
Dec 2015
$150
House Payment
Dec 2015
$3000
Pay


http://bank1.com/billpay.aspx
Identified by VeriSign
Bank 1 Online
Bank1
Welcome, Pedro
My Settings | Security | Secure Message(s) | ATMs/Branches | Help | Logout
Search or ask a question
MY ACCOUNTS
CHECKING & SAVINGS
LOANS & CREDIT
ONLINE SERVICES
INVESTMENTS
INSURANCE
Thursday, October 23, 2014 11:57 AM (Pacific)
Printer Friendly
Quick Links
Balances
BillPay
X
Select an account to pay with:
Bank1
Ok
Cancel
User Other
Get New
House Payment
Dec 2015
$3000
Pay


http://bank1.com/billpay.aspx
Identified by VeriSign
Bank 1 Online
Bank1
Welcome, Pedro
My Settings | Security | Secure Message(s) | ATMs/Branches | Help | Logout
Search or ask a question
MY ACCOUNTS
CHECKING & SAVINGS
LOANS & CREDIT
ONLINE SERVICES
INVESTMENTS
INSURANCE
Thursday, October 23, 2014 11:57 AM (Pacific)
Printer Friendly
Quick Links
Balances
BillPay
X
Select one of our partners to add new payment type:
Other Card
Ok
Cancel
House Payment
Dec 2015
$3000
Pay

http://othercard.com/payment/application.aspx

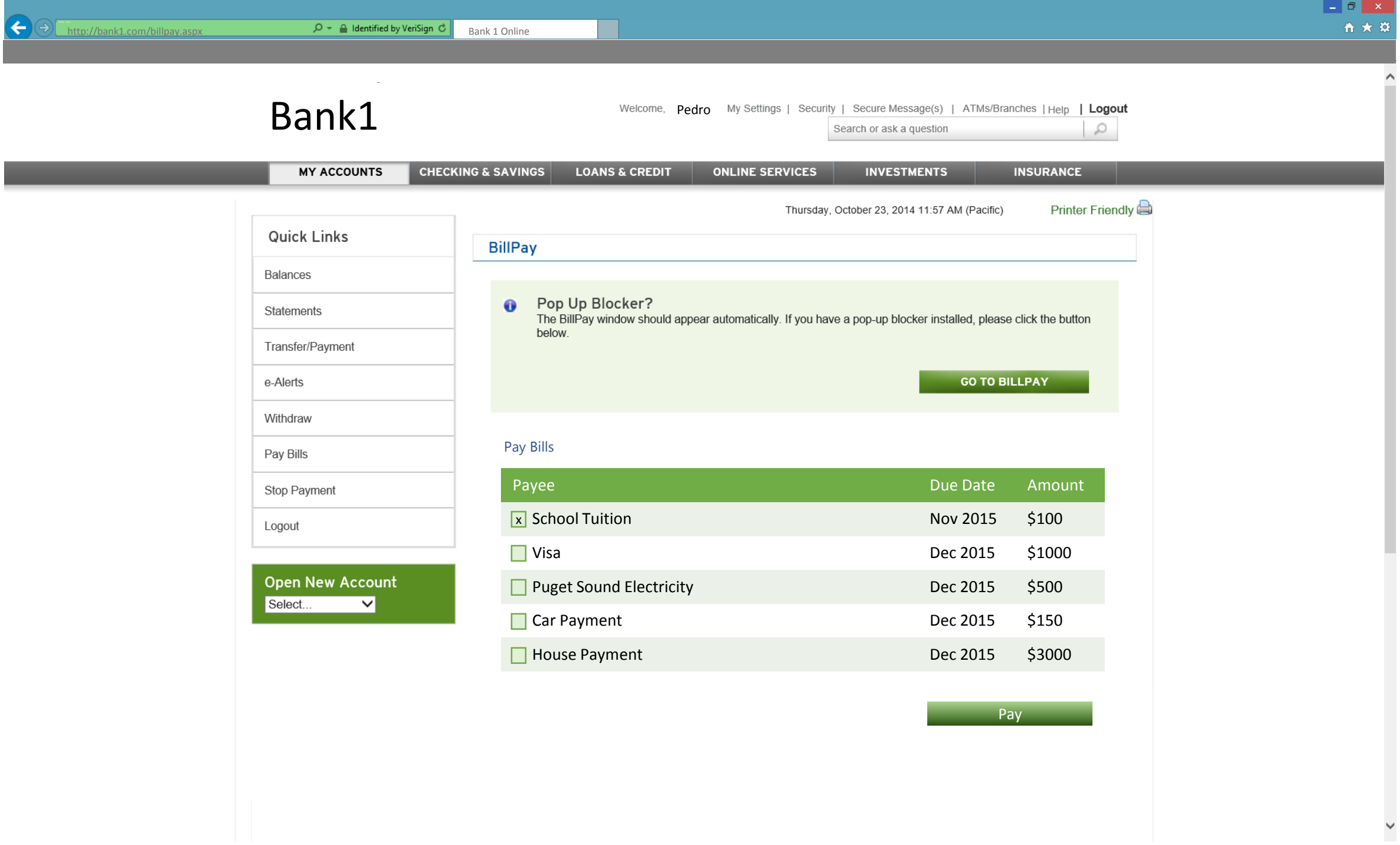
Bank 1 Online

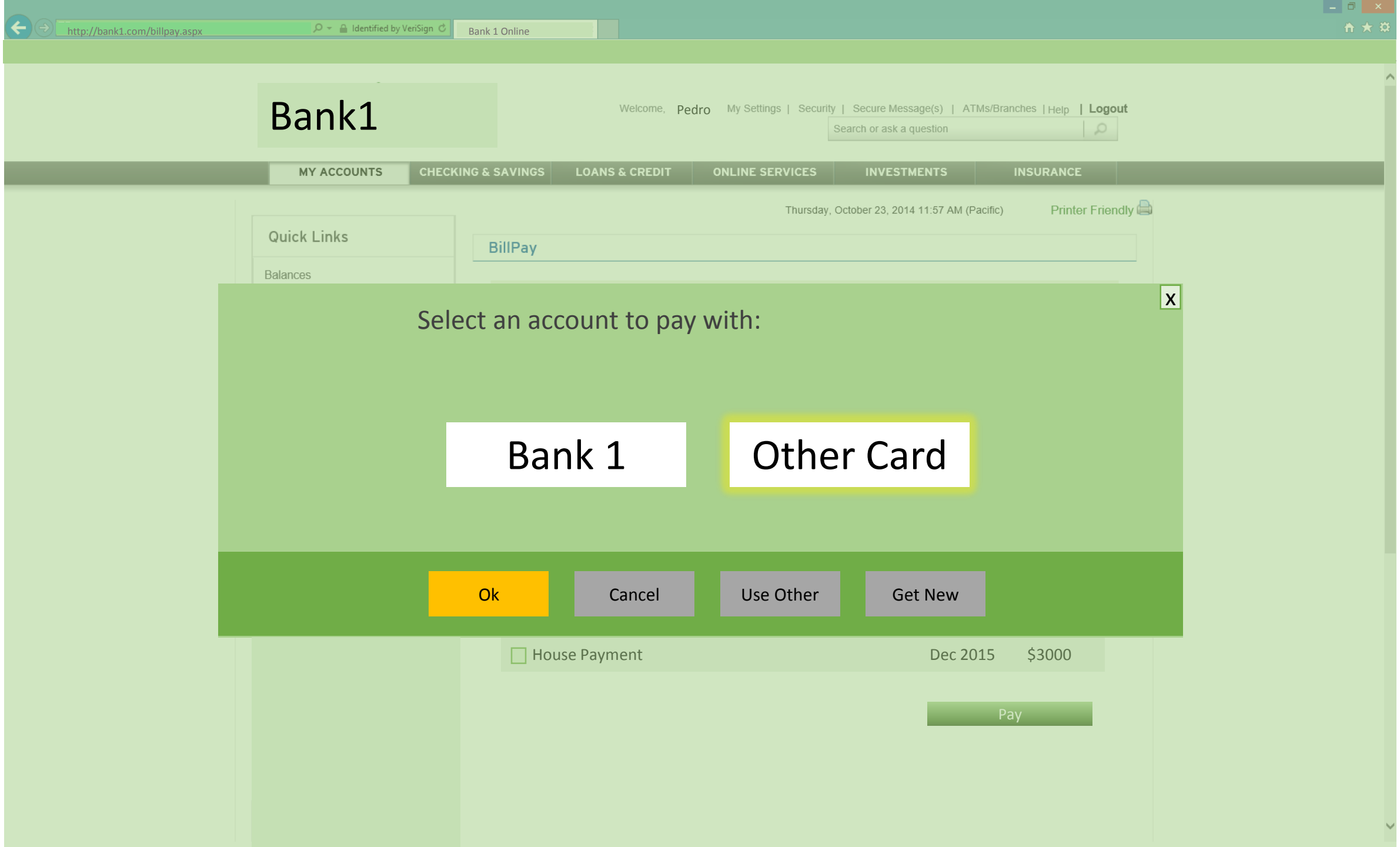
Other Card

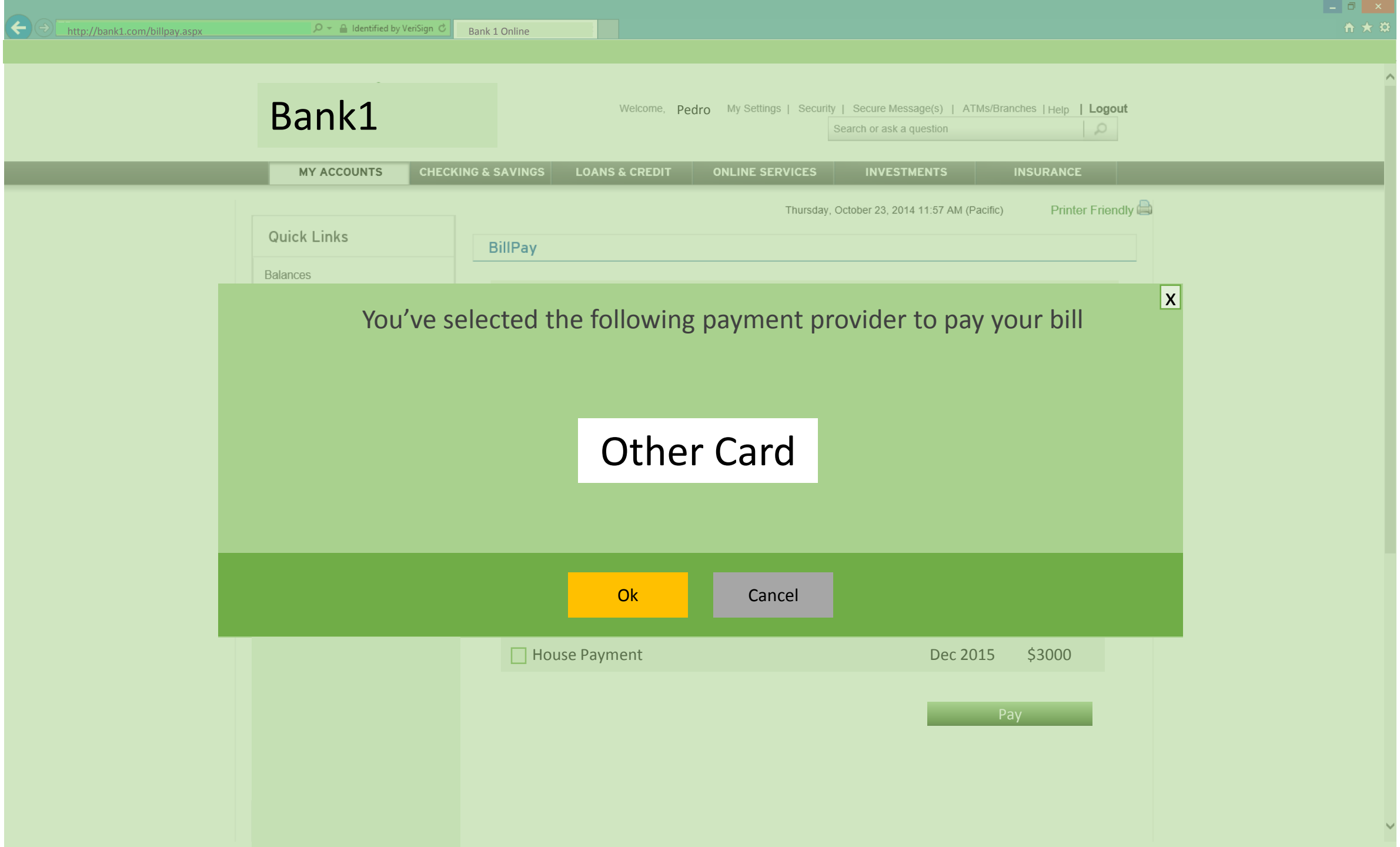
Welcome to Other Card payment options

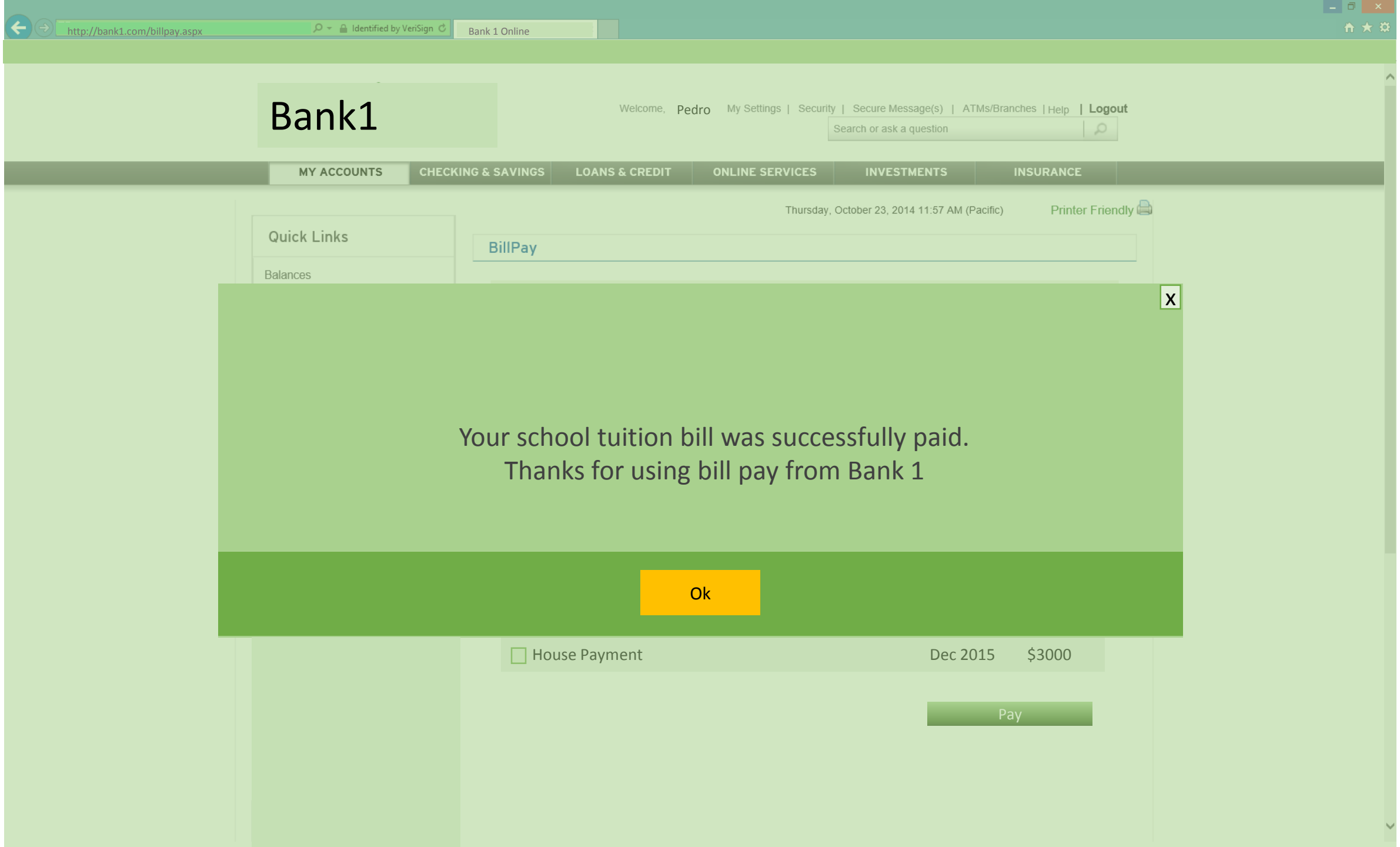
Sign Up

Follow the Other Card flow to obtain a certificate that can be used at Bank 1


http://bank1.com/billpay.aspx
Identified by VeriSign
Bank 1 Online
Bank1
Welcome, Pedro
My Settings | Security | Secure Message(s) | ATMs/Branches | Help | Logout
Search or ask a question
MY ACCOUNTS
CHECKING & SAVINGS
LOANS & CREDIT
ONLINE SERVICES
INVESTMENTS
INSURANCE
Thursday, October 23, 2014 11:57 AM (Pacific)
Printer Friendly
Quick Links
Balances
Statements
Transfer/Payment
e-Alerts
Withdraw
Pay Bills
Stop Payment
Logout
Open New Account
Select...
BillPay
Pop Up Blocker?
The BillPay window should appear automatically. If you have a pop-up blocker installed, please click the button below.
GO TO BILLPAY
Pay Bills
Payee
Due Date
Amount
x School Tuition
Nov 2015
$100
Visa
Dec 2015
$1000
Puget Sound Electricity
Dec 2015
$500
Car Payment
Dec 2015
$150
House Payment
Dec 2015
$3000
Pay


http://bank1.com/billpay.aspx
Identified by VeriSign
Bank 1 Online
Bank1
Welcome, Pedro
My Settings | Security | Secure Message(s) | ATMs/Branches | Help | Logout
Search or ask a question
MY ACCOUNTS
CHECKING & SAVINGS
LOANS & CREDIT
ONLINE SERVICES
INVESTMENTS
INSURANCE
Thursday, October 23, 2014 11:57 AM (Pacific)
Printer Friendly
Quick Links
Balances
BillPay
X
Select an account to pay with:
Bank 1
Other Card
Ok
Cancel
Use Other
Get New
House Payment
Dec 2015
$3000
Pay


http://bank1.com/billpay.aspx
Identified by VeriSign
Bank 1 Online
Bank1
Welcome, Pedro
My Settings | Security | Secure Message(s) | ATMs/Branches | Help | Logout
Search or ask a question
MY ACCOUNTS
CHECKING & SAVINGS
LOANS & CREDIT
ONLINE SERVICES
INVESTMENTS
INSURANCE
Thursday, October 23, 2014 11:57 AM (Pacific)
Printer Friendly
Quick Links
Balances
BillPay
X
You've selected the following payment provider to pay your bill
Other Card
Ok
Cancel
House Payment
Dec 2015
$3000
Pay


http://bank1.com/billpay.aspx
Identified by VeriSign
Bank 1 Online
Bank1
Welcome, Pedro
My Settings | Security | Secure Message(s) | ATMs/Branches | Help | Logout
Search or ask a question
MY ACCOUNTS
CHECKING & SAVINGS
LOANS & CREDIT
ONLINE SERVICES
INVESTMENTS
INSURANCE
Thursday, October 23, 2014 11:57 AM (Pacific)
Printer Friendly
Quick Links
Balances
BillPay
X
Your school tuition bill was successfully paid.
Thanks for using bill pay from Bank 1
Ok
House Payment
Dec 2015
$3000
Pay

API Proposal for managing and using Keys and Certificates

WebCrypto API Extensions

Additions to SubtleCrypto

```
partial interface SubtleCrypto {
        Promise<any> signExt(
                AlgorithmIdentifier algorithm,
                TokenKey key,
                CryptoOperationData data,
                DOMString extraInfo
        );
        Promise<any> generateKey(
                AlgorithmIdentifier algorithm,
                boolean extractable,
                sequence<KeyUsage> keyUsages,
                KeyMetadata metadata);
        // returns a CryptoKey or KeyPair
};
```

New Interfaces

```
Interface CryptoKeys {
        Promise<any> getKey (
                AlgorithmIdentifier algorithm,
                sequence<KeyUsage> keyUsages
        );
        Promise<any> getCertificate (
                DOMString issuer,
                DOMString subject
        );
};
partial interface Window {
        readonly    attribute CryptoKeys cryptokeys;
};
```

```
interface Certificate {
        readonly attribute DOMString issuer;
        readonly attribute DOMString serial;
        readonly attribute DOMString subjectName;
        readonly attribute Date expiration;
        readonly attribute KeyPair keys;
};
interface TokenKey : CryptoKey {
        readonly attribute KeyMetadata metadata;
};
dictionary KeyMetadata {
        required DOMString userAgentString;
        readonly attribute DOMString domainName;
};
```

Sample Program

Part #1 – Key Generation

```
var myCrypto = window.crypto.subtle;
function provisionKey(desiredAlg) {
        return myCrypto.generateKey(desiredAlg, false, [‘sign’, ‘verify’],
            ‘{userAgentString:”Your favorite key”,user:”batman”;status:”always prepared”}’).then(
        function (keypair) {
            /* Clone to local storage */
            return myCrypto.export(“jwk”, keypair.publicKey).then(
                function (keyObject) {
                        /* Share/publish the public key. */
                 });
        });
}
```

Part #2 – Key Discovery & Selection

```
function findKeyAndDoAuthentication(desiredAlg, keyUsages) {
    return window.cryptokeys.getKey(desiredAlg, keyUsages).then(
    /* User Select key from UA key List */
    function (key) {
        /* Clone key to persisted storage if desired. */
        return window.crypto.subtle.signExt(alg, key, data,
            {userAgentString:“Sign this please”}).then(
        function (signature) {
            /* Send to server for verification */
        });
    });
}
```

Related Work

- WebCrypto Key Discovery
- Web Certificate APIs
- U2F JavaScript API
- U2F WebCrypto algorithm
- UAF JavaScript API
- Enterprise.platformKeys API
- Proposal for Secure Element support

Appendix

Certificate Usage Flow

*** Bold operations are executed by the UA**