Your Bank's Digital Side Door

@sdanndev

SECURITY INNOVATION

“Because that’s where the money is.”

Willie Sutton, Bank Robber

Why does my bank website require my 2-factor token, but pulling my transactions into Quicken does not?

Personal Financial Management

PFM

Personal Financial Management (PFM)

Quicken

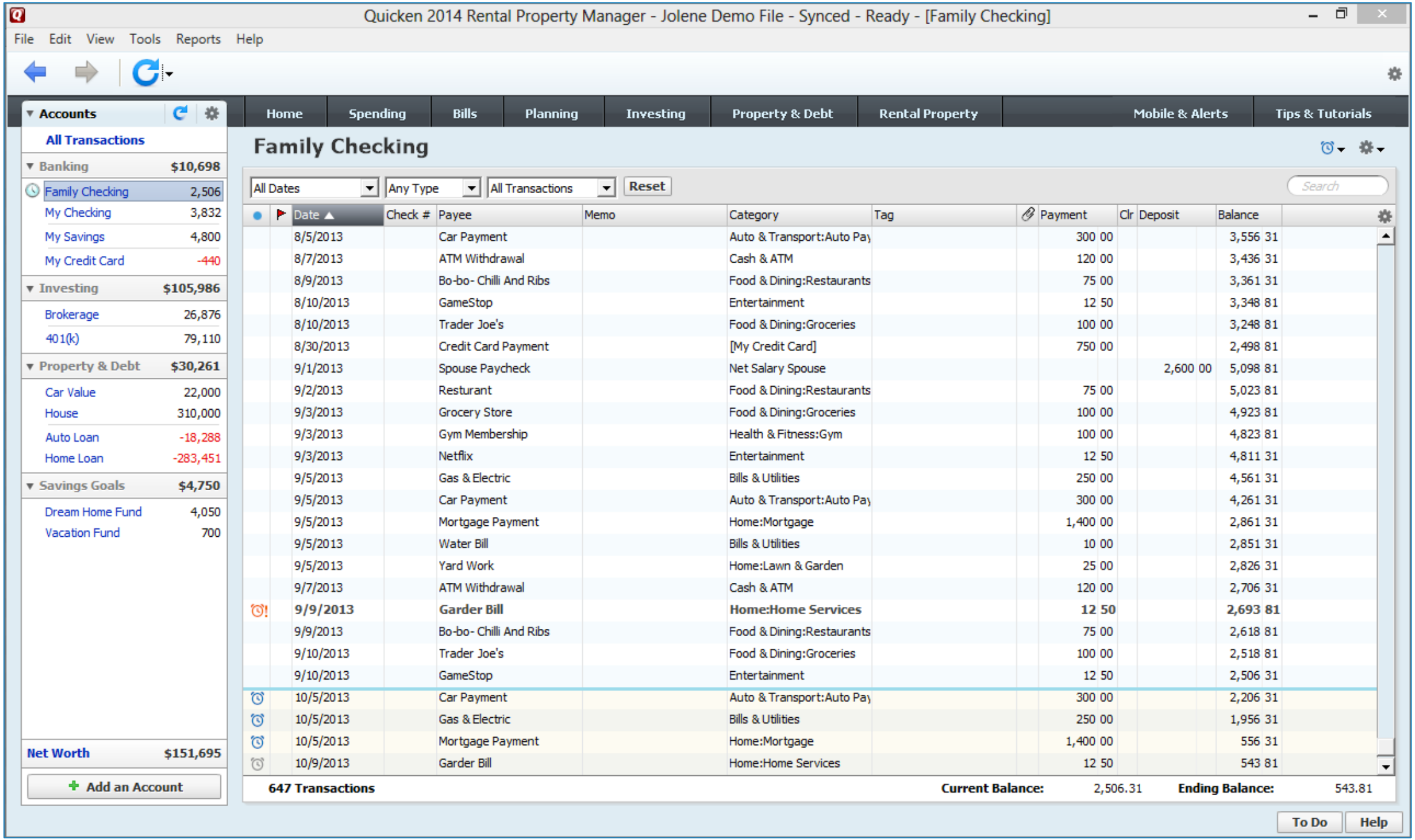
PERSONAL CAPITAL

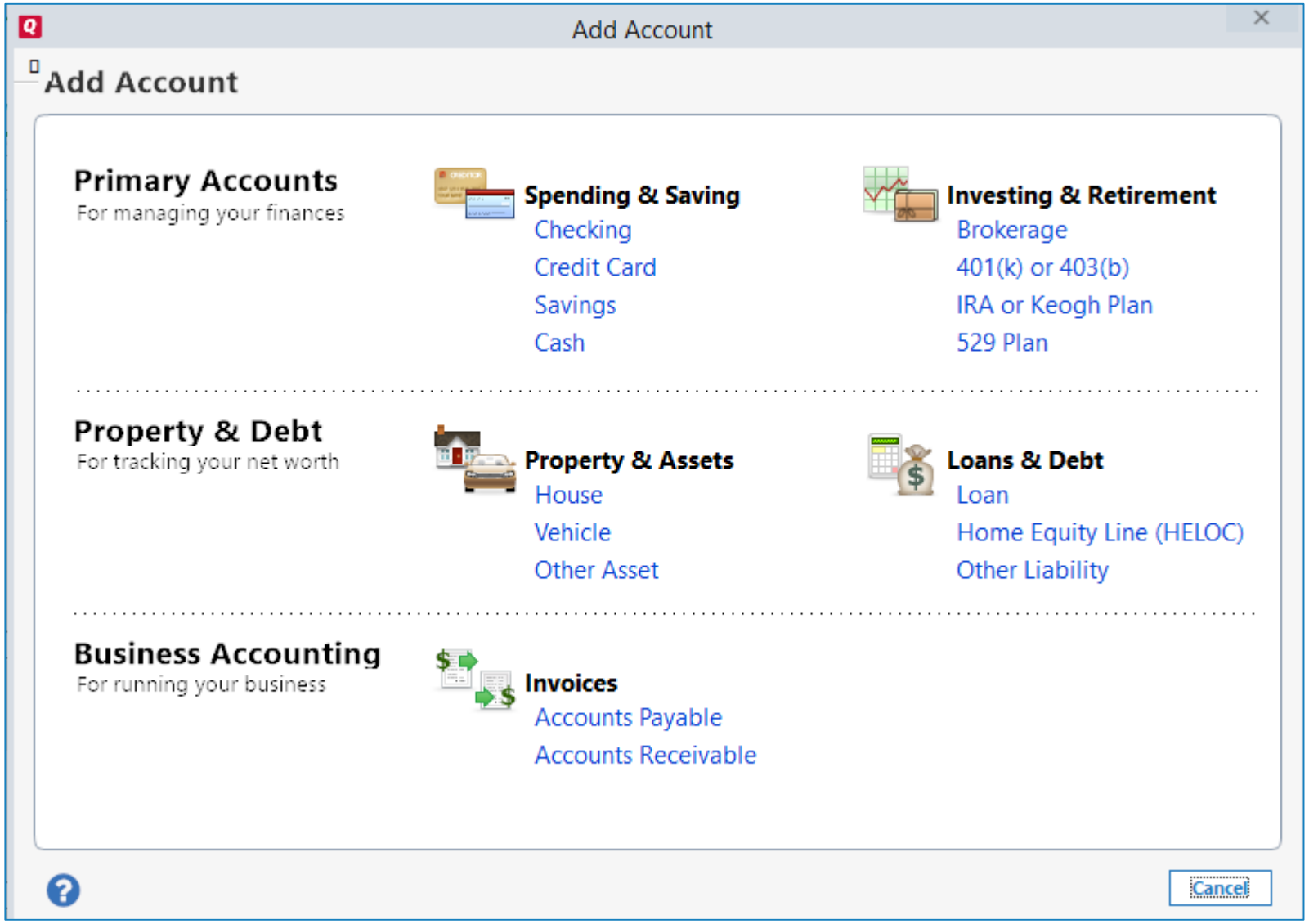
intuit QuickBooks

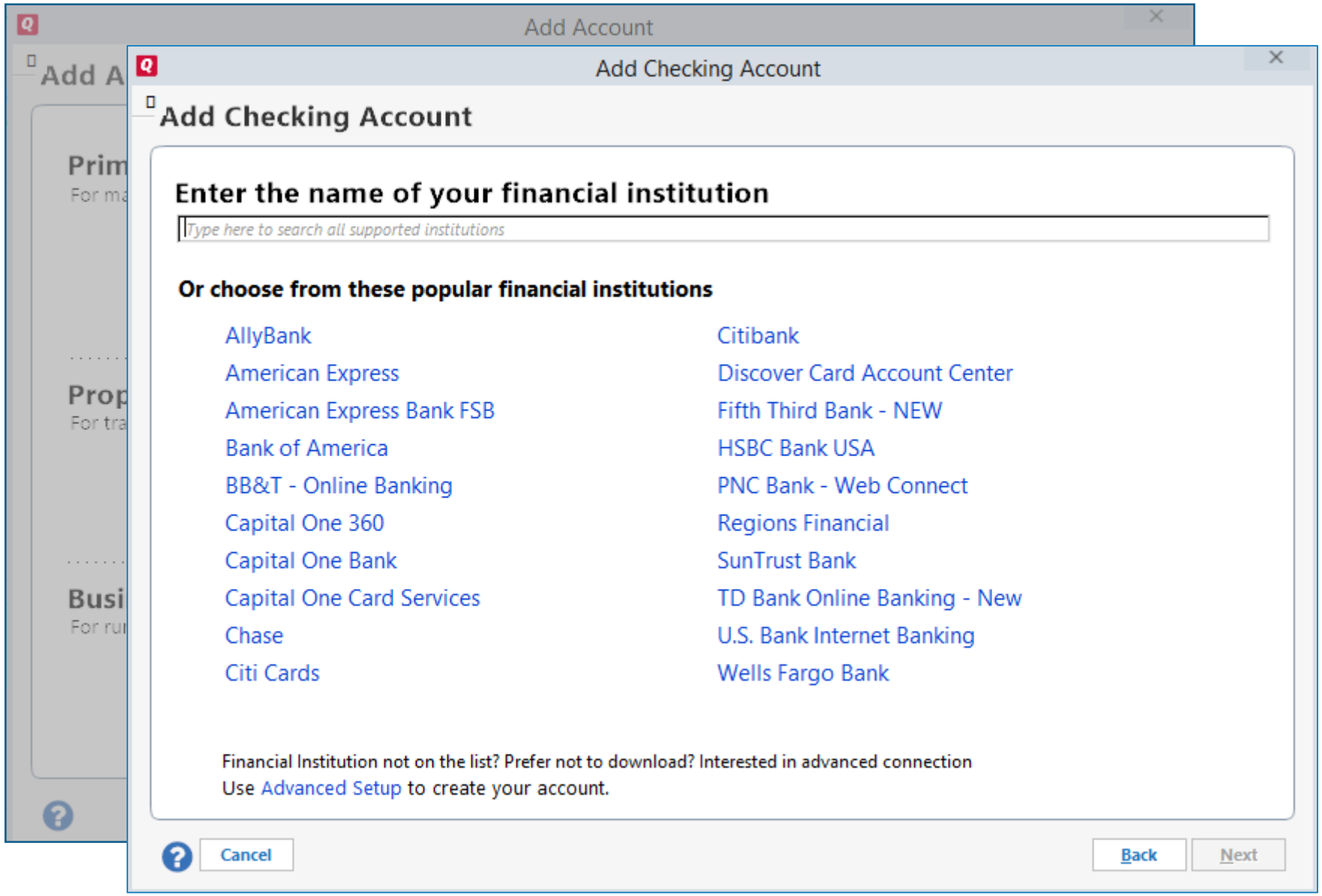
Microsoft Money

GnuCash
Free Accounting Software

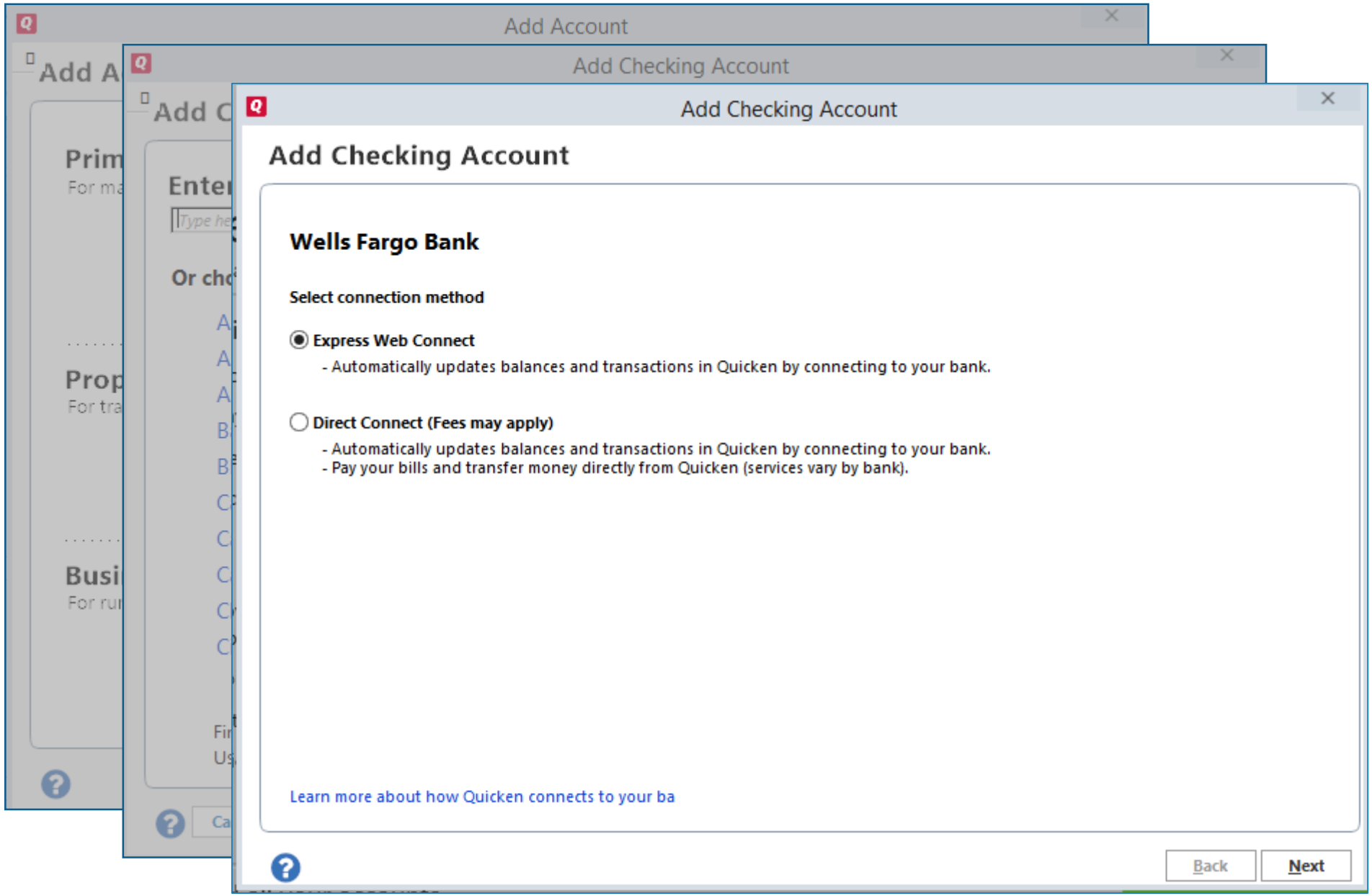
mint.com


Quicken 2014 Rental Property Manager - Jolene Demo File - Synced - Ready - [Family Checking]
File Edit View Tools Reports Help
Accounts
All Transactions
Banking $10,698
Family Checking 2,506
My Checking 3,832
My Savings 4,800
My Credit Card -440
Investing $105,986
Brokerage 26,876
401(k) 79,110
Property & Debt $30,261
Car Value 22,000
House 310,000
Auto Loan -18,288
Home Loan -283,451
Savings Goals $4,750
Dream Home Fund 4,050
Vacation Fund 700
Net Worth $151,695
Add an Account
Home Spending Bills Planning Investing Property & Debt Rental Property Mobile & Alerts Tips & Tutorials
Family Checking
All Dates Any Type All Transactions Reset Search
Date Check # Payee Memo Category Tag Payment Clr Deposit Balance
8/5/2013 Car Payment Auto & Transport:Auto Pay 300 00 3,556 31
8/7/2013 ATM Withdrawal Cash & ATM 120 00 3,436 31
8/9/2013 Bo-bo- Chilli And Ribs Food & Dining:Restaurants 75 00 3,361 31
8/10/2013 GameStop Entertainment 12 50 3,348 81
8/10/2013 Trader Joe's Food & Dining:Groceries 100 00 3,248 81
8/30/2013 Credit Card Payment [My Credit Card] 750 00 2,498 81
9/1/2013 Spouse Paycheck Net Salary Spouse 2,600 00 5,098 81
9/2/2013 Resturant Food & Dining:Restaurants 75 00 5,023 81
9/3/2013 Grocery Store Food & Dining:Groceries 100 00 4,923 81
9/3/2013 Gym Membership Health & Fitness:Gym 100 00 4,823 81
9/3/2013 Netflix Entertainment 12 50 4,811 31
9/5/2013 Gas & Electric Bills & Utilities 250 00 4,561 31
9/5/2013 Car Payment Auto & Transport:Auto Pay 300 00 4,261 31
9/5/2013 Mortgage Payment Home:Mortgage 1,400 00 2,861 31
9/5/2013 Water Bill Bills & Utilities 10 00 2,851 31
9/5/2013 Yard Work Home:Lawn & Garden 25 00 2,826 31
9/7/2013 ATM Withdrawal Cash & ATM 120 00 2,706 31
9/9/2013 Garder Bill Home:Home Services 12 50 2,693 81
9/9/2013 Bo-bo- Chilli And Ribs Food & Dining:Restaurants 75 00 2,618 81
9/10/2013 Trader Joe's Food & Dining:Groceries 100 00 2,518 81
9/10/2013 GameStop Entertainment 12 50 2,506 31
10/5/2013 Car Payment Auto & Transport:Auto Pay 300 00 2,206 31
10/5/2013 Gas & Electric Bills & Utilities 250 00 1,956 31
10/5/2013 Mortgage Payment Home:Mortgage 1,400 00 556 31
10/9/2013 Garder Bill Home:Home Services 12 50 543 81
647 Transactions
Current Balance: 2,506.31
Ending Balance: 543.81
To Do Help

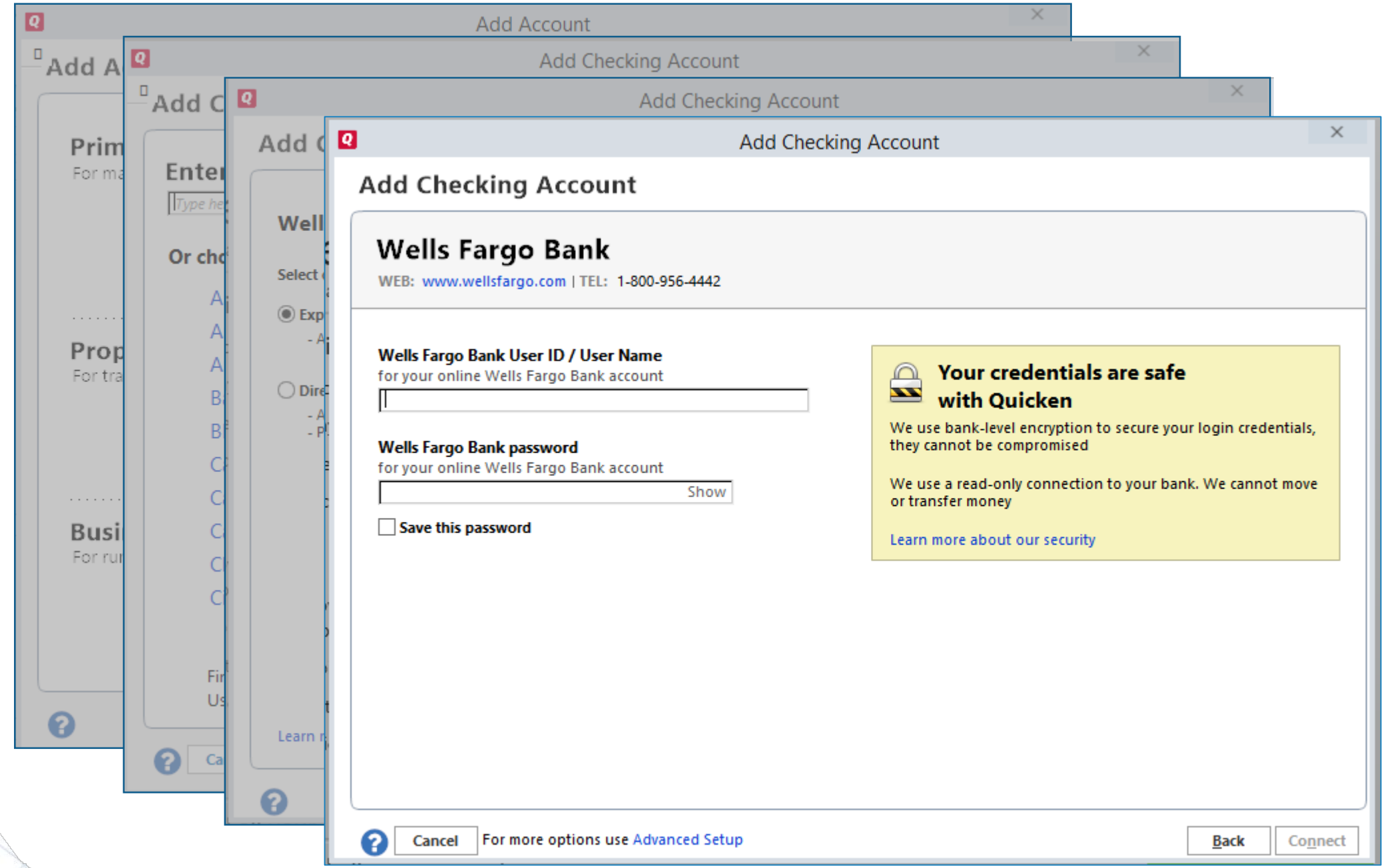




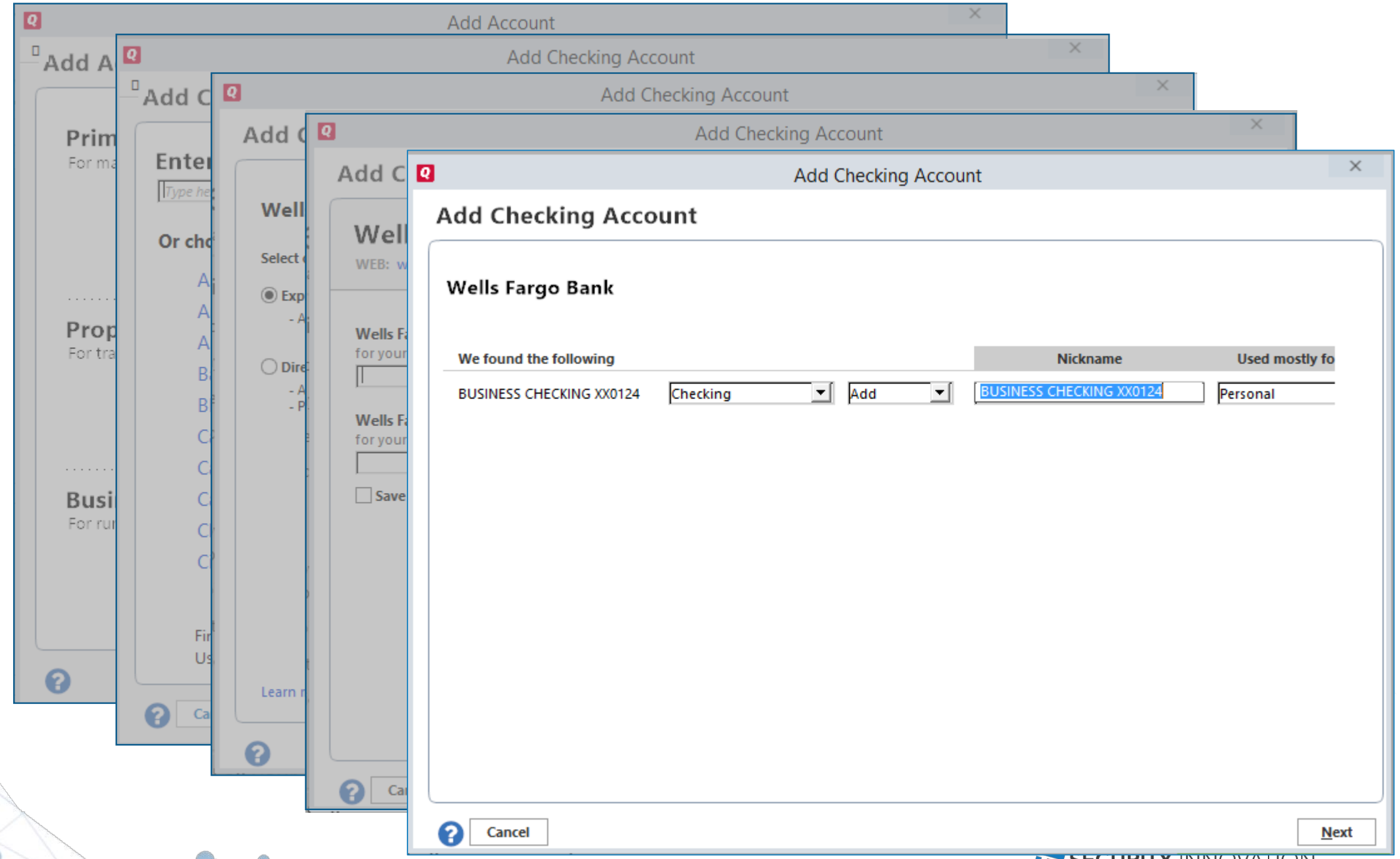
SECURITY INNOVATION

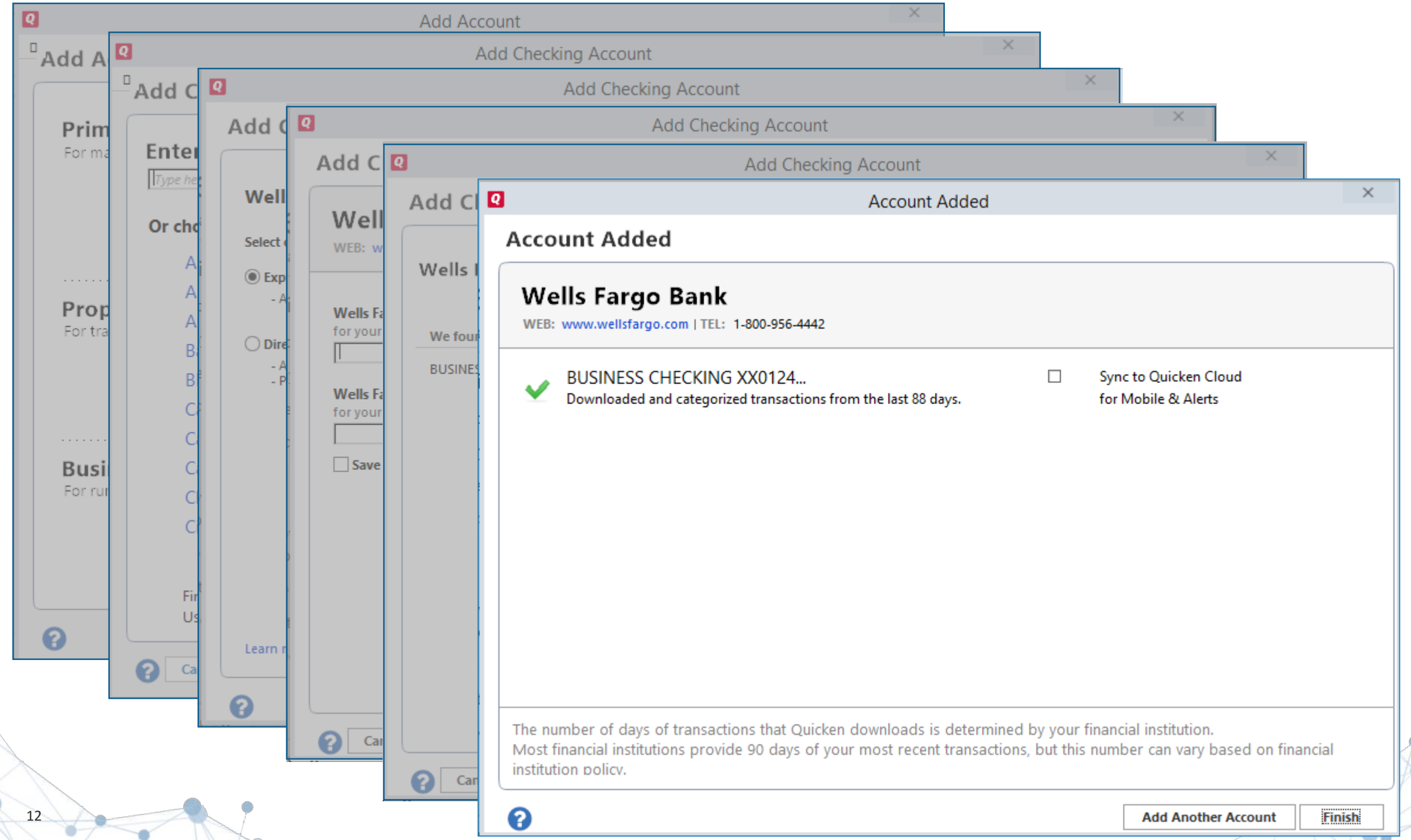


SECURITY INNOVATION



SECURITY INNOVATION


Add Account
Add Checking Account
Add Checking Account
Add Checking Account
Add Checking Account
Add Checking Account
Wells Fargo Bank
We found the following
Nickname
Used mostly fo
BUSINESS CHECKING XX0124
Checking
Add
BUSINESS CHECKING XX0124
Personal
Cancel
Next


Add Account
Add Checking Account
Add Checking Account
Add Checking Account
Add Checking Account
Account Added
Account Added
Wells Fargo Bank
WEB: www.wellsfargo.com | TEL: 1-800-956-4442
BUSINESS CHECKING XX0124...
Downloaded and categorized transactions from the last 88 days.
Sync to Quicken Cloud
for Mobile & Alerts
The number of days of transactions that Quicken downloads is determined by your financial institution.
Most financial institutions provide 90 days of your most recent transactions, but this number can vary based on financial institution policy.
Add Another Account
Finish

Quicken/Quickbooks Connection Types

Web Connect

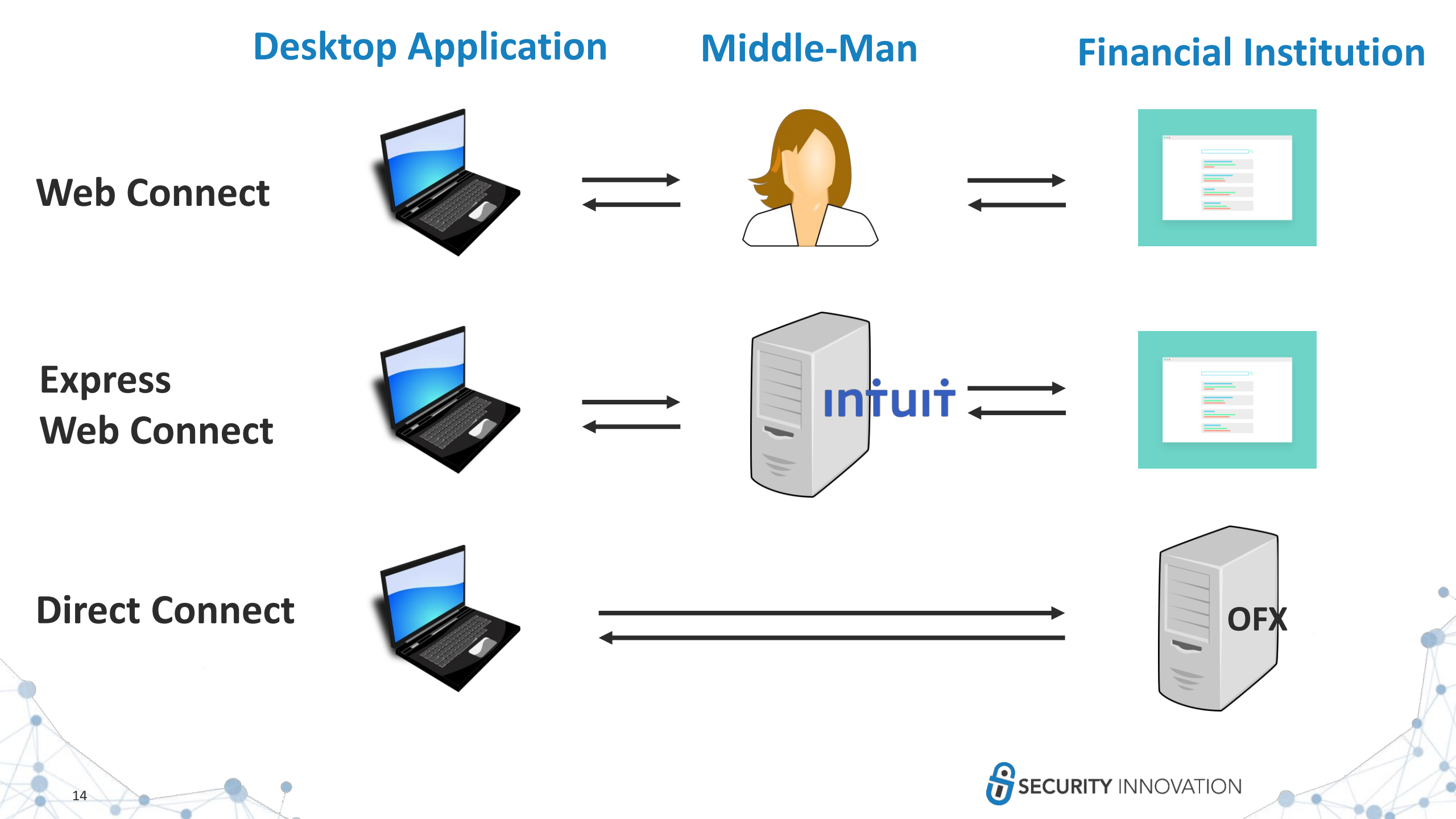
- Unidirectional
- Manual
- Download a file
- OFX file format

Express Web Connect

- Unidirectional
- Programmatic
- Screen scrape
- Private web service

Direct Connect

- Bidirectional
- Programmatic
- Structured query
- OFX protocol

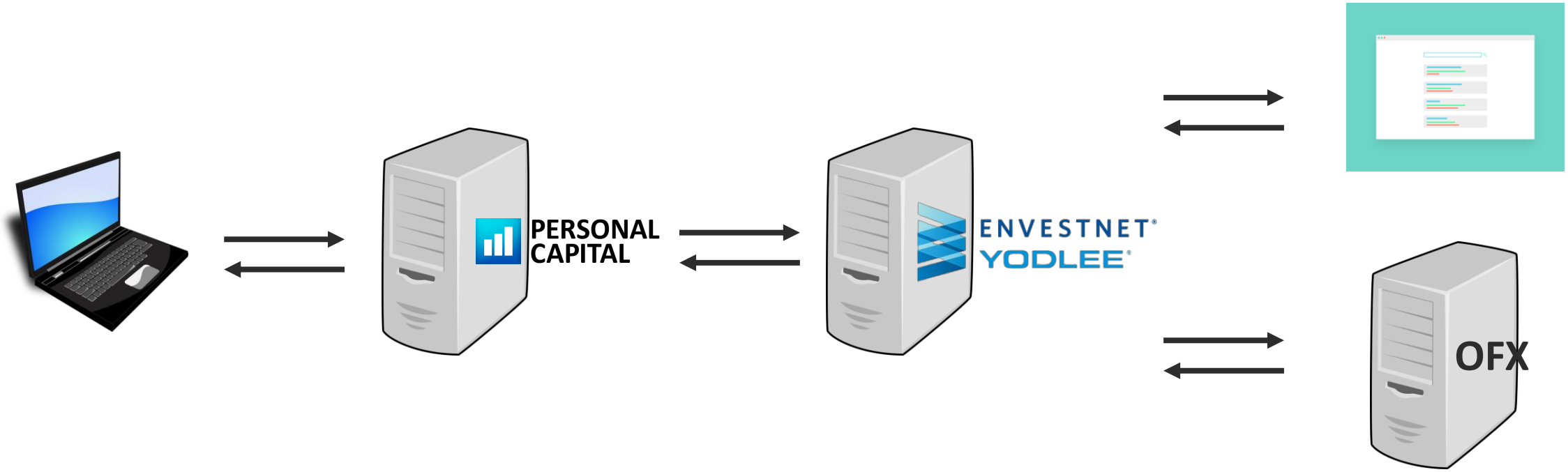


Account Aggregation Service / API

Web Application

Middle-Man

Financial Institution



Personal Threat Model

- Assets
  - Checking account
  - Brokerage account
- Threats
  - Credentials are stolen
  - Accounts are accessible without credentials

@mrvaughan: https://youtu.be/PIwvxSZj5e8

Lack of Least Privilege

- Users have 1 set of bank credentials
  - Full read / write access to all accounts at financial institution
- Plain text password is shared with and stored by aggregators
- Tokenized application-based access control (OAuth) is needed

Open Financial Exchange (OFX)

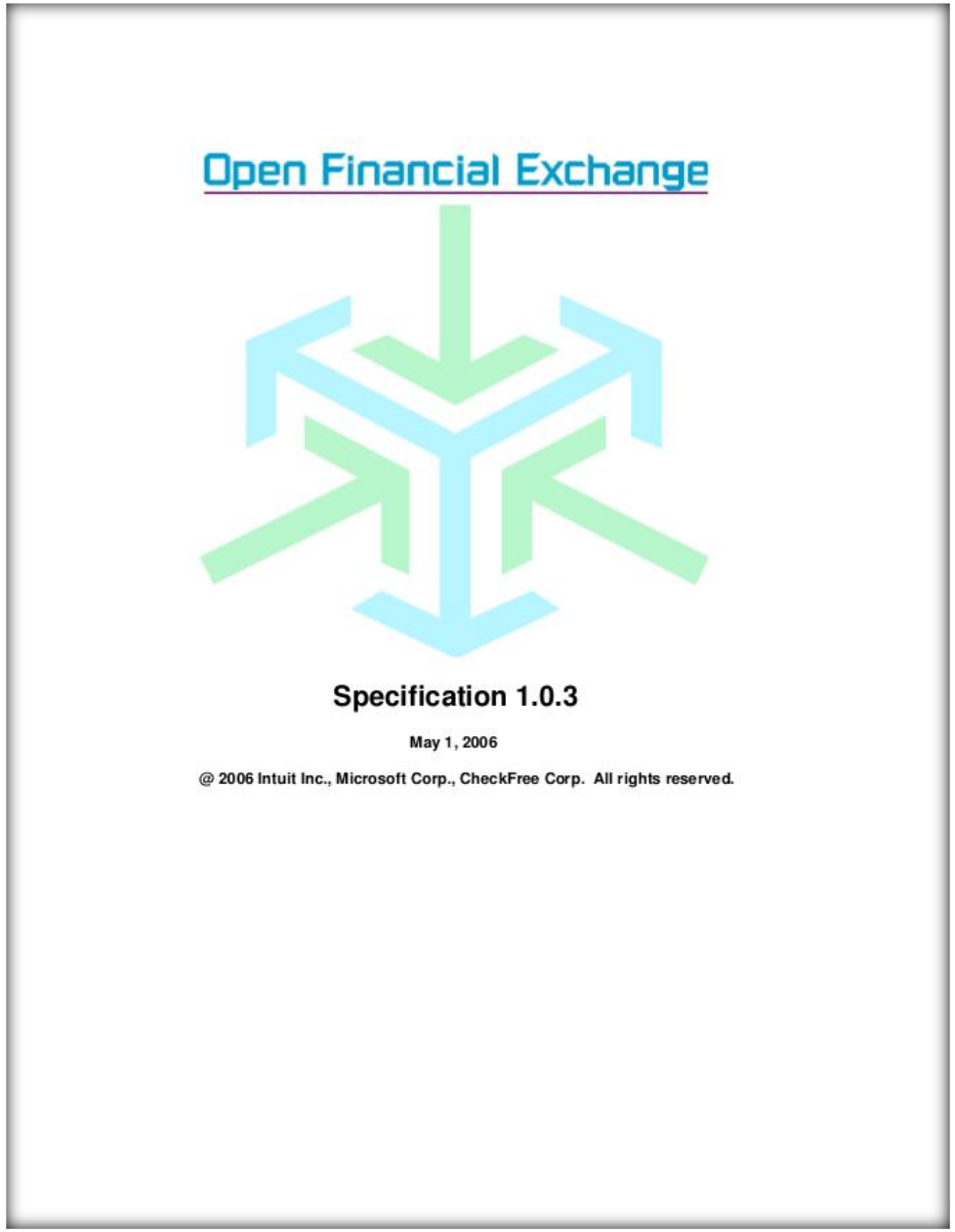
aka Direct Connect

OFX Functionality - Financial

Banking	Investment	Credit Cards	Transfers
• Checking • Savings • CDs • Loans	• IRA • 401k • Holdings • Equity Prices	• Transactions	• Bill Pay • Intrabank • Interbank • Wire Funds

OFX Functionality - Miscellaneous

- Enrollment
  - Setup online access
  - Password Reset
- FI Profile
  - Like a homepage
- Email
  - Messages and Notifications
- Synchronization
  - Ensure multiple clients receive 1-time messages.
- Image download
  - JPEG, TIFF, PNG, PDF
- Bill Presentment
  - For 3rd parties


Open Financial Exchange
Specification 1.0.3
May 1, 2006
@ 2006 Intuit Inc., Microsoft Corp., CheckFree Corp. All rights reserved.

www.ofx.org

Request

```
POST /cgi/ofx HTTP/1.1
Accept: */*
Content-Type: application/x-ofx
Date: Fri, 16 Jun 2018 21:12:27 GMT
User-Agent: InetClntApp/3.0
Content-Length: 570
Connection: close

OFXHEADER:100
DATA:OFXSGML
VERSION:103
SECURITY:NONE
ENCODING:USASCII

<OFX>
    <SIGNONMSGSRQV1>
        <SONRQ>
            <DTCLIENT>20060321083010
            <USERID>12345
            <USERPASS>MyPassword
            <LANGUAGE>ENG
            <FI>
                <ORG>ABC
                <FID>000111222
            </FI>
            <APPID>MyApp
        </SONRQ>
    </SIGNONMSGSRQV1>
    ... <!--Other message sets-->
</OFX>
```

Response

```
HTTP/1.1 200 OK
Date: Fri, 16 Jun 2018 21:12:30 GMT
Content-Type: application/x-ofx
Connection: Keep-Alive
Content-Length: 2399

OFXHEADER:100
DATA:OFXSGML
VERSION:103
SECURITY:NONE
ENCODING:USASCII

<OFX>
    <SIGNONMSGSRSV1>
        <SONRS>
            <STATUS>
                <CODE>0
                <SEVERITY>INFO
                <MESSAGE>Success
            </STATUS>
            <DTSERVER>20060321083445
            <LANGUAGE>ENG
            <FI>
                <ORG>ABC
                <FID>000111222
            </FI>
        </SONRS>
    </SIGNONMSGSRSV1>
    ... <!--All other transaction responses-->
</OFX>
```

Request

```
OFXHEADER:100
DATA:OFXSGML
VERSION:103
SECURITY:NONE
ENCODING:USASCII

<OFX>
    <SIGNONMSGSRQV1>
        <SONRQ>
            <DTCLIENT>20060321083010
            <USERID>12345
            <USERPASS>MyPassword
            <LANGUAGE>ENG
            <FI>
                <ORG>ABC
                <FID>000111222
            </FI>
            <APPID>MyApp
        </SONRQ>
    </SIGNONMSGSRQV1>
    ... <!--Other message sets-->
</OFX>
```

Response

```
OFXHEADER:100
DATA:OFXSGML
VERSION:103
SECURITY:NONE
ENCODING:USASCII

<OFX>
    <SIGNONMSGSRSV1>
        <SONRS>
            <STATUS>
                <CODE>0
                <SEVERITY>INFO
                <MESSAGE>Success
            </STATUS>
            <DTSERVER>20060321083445
            <LANGUAGE>ENG
            <FI>
                <ORG>ABC
                <FID>000111222
            </FI>
        </SONRS>
    </SIGNONMSGSRSV1>
    ... <!--All other transaction responses-->
</OFX>
```

Profile <PROFRQ> *anonymous*

<PROFRS> Supported features

Account Info <ACCTINFORQ> *user:pass*

<ACCTINFORS> List of available accounts

Bank Statement <STMTTRNRQ> *user:pass*

<STMTTRNRS> List of transactions

Request

```
OFXHEADER:100
DATA:OFXSGML
VERSION:103
SECURITY:NONE
ENCODING:USASCII

<OFX>
    <SIGNONMSGSRQV1>
        ... <!--Anonymous sign on-->
    </SIGNONMSGSRQV1>
    <PROFMSGSRQV1>
        <PROFTRNRQ>
            <TRNUID>5A59A330-7CEC-1000-A761
            <PROFRQ>
                <CLIENTROUTING>MSGSET
                <DTPROFUP>19900101
            </PROFRQ>
        </PROFTRNRQ>
    </PROFMSGSRQV1>
</OFX>
```

Response

```
OFXHEADER:100
DATA:OFXSGML
VERSION:103
SECURITY:NONE
ENCODING:USASCII

<OFX>
    ... <!--Anonymous sign on success-->
    <BANKMSGSET>
        <BANKMSGSETV1>
            <MSGSETCORE>
                <URL>https://o.bank.org/ofx.asp
                <LANGUAGE>ENG
                <SPNAME>Corillian Corp
            </MSGSETCORE>
            <XFERPROF>
                <PROCENDTM>235959[0:GMT]
                <CANSCHED>Y
                <CANRECUR>N
                <CANMODXFERS>N
            </XFERPROF>
        </BANKMSGSETV1>
    </BANKMSGSET>
</OFX>
```

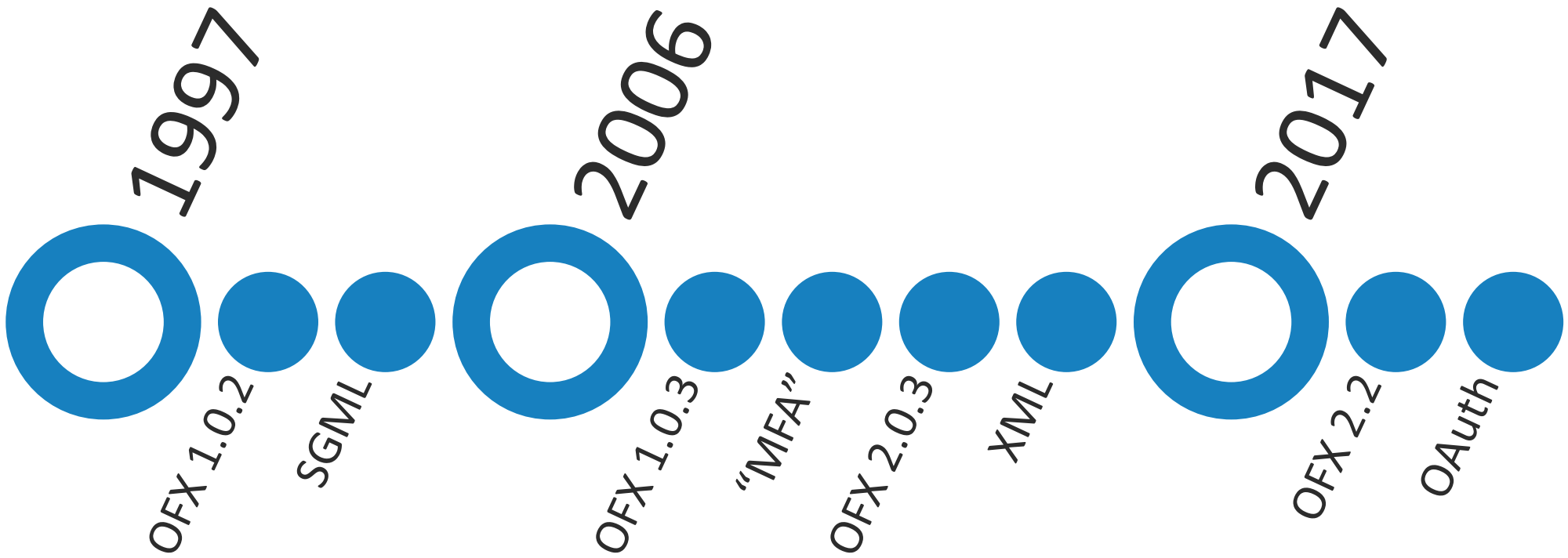
Request

```
OFXHEADER:100
DATA:OFXSGML
VERSION:103
SECURITY:NONE
ENCODING:USASCII

<OFX>
    <SIGNONMSGSRQV1>
        ... <!--Anonymous sign on-->
    </SIGNONMSGSRQV1>
    <PROFMSGSRQV1>
        <PROFTRNRQ>
            <TRNUID>5A59A330-7CEC-1000-A761
            <PROFRQ>
                <CLIENTROUTING>MSGSET
                <DTPROFUP>19900101
            </PROFRQ>
        </PROFTRNRQ>
    </PROFMSGSRQV1>
</OFX>
```

Response

```
OFXHEADER:100
DATA:OFXSGML
VERSION:103
SECURITY:NONE
ENCODING:USASCII

<OFX>
    ... <!--Anonymous sign on success-->
    <PROFMSGSRSV1>
        <PROFTRNRS>
            <PROFRS>
                <FINAME>Bank
                <ADDR1>123 Muholland Drive
                <CITY>Las Vegas
                <STATE>NV
                <POSTALCODE>89109
                <COUNTRY>USA
                <CSPHONE>206-439-5700
                <URL>http://www.bank.org
                <EMAIL>info@bank.org
            </PROFRS>
        </PROFTRNRS>
    </PROFMSGSRSV1>
</OFX>
```

OFX Protocol Specification



SECURITY INNOVATION

OFX 1.0.x

1.0.2 - 1997

- BASIC authentication
  - User:Pass sent plaintext
  - Over HTTPS
- Suggests SSN for username
- SGML

1.0.3 - 2006

- Added “MFA”

OFX 2.x.x

2.0.3 - 2006

- BASIC authentication
  - User:Pass sent plaintext
  - Over HTTPS
- Added “MFA”
- XML
- Taxes (1099, W2)

2.2.0 - 2017

- Token-based Authentication
  - OAuth

Multi-Factor Authentication (MFA)

Know	Have	Are

• Password
• PIN
• Security Question
	• Token
	  • Hardware
	  • Software
	• PKI Certificate
	• Smart Card
		• Biometric
		• Behavior

2-Step Authentication

- Password + out-of-band mechanism
  - 6 digit string
    - SMS
    - Push notification
    - Software token

OFX “MFA”

Security Question

- <USERCRED1>
  - Free form field required by server
  - Server defines label
  - Ex: “Mother’s maiden name.”

- <MFACHALLENGE>
  - Security questions
  - Hard coded list
  - Ex: “Favorite color.”

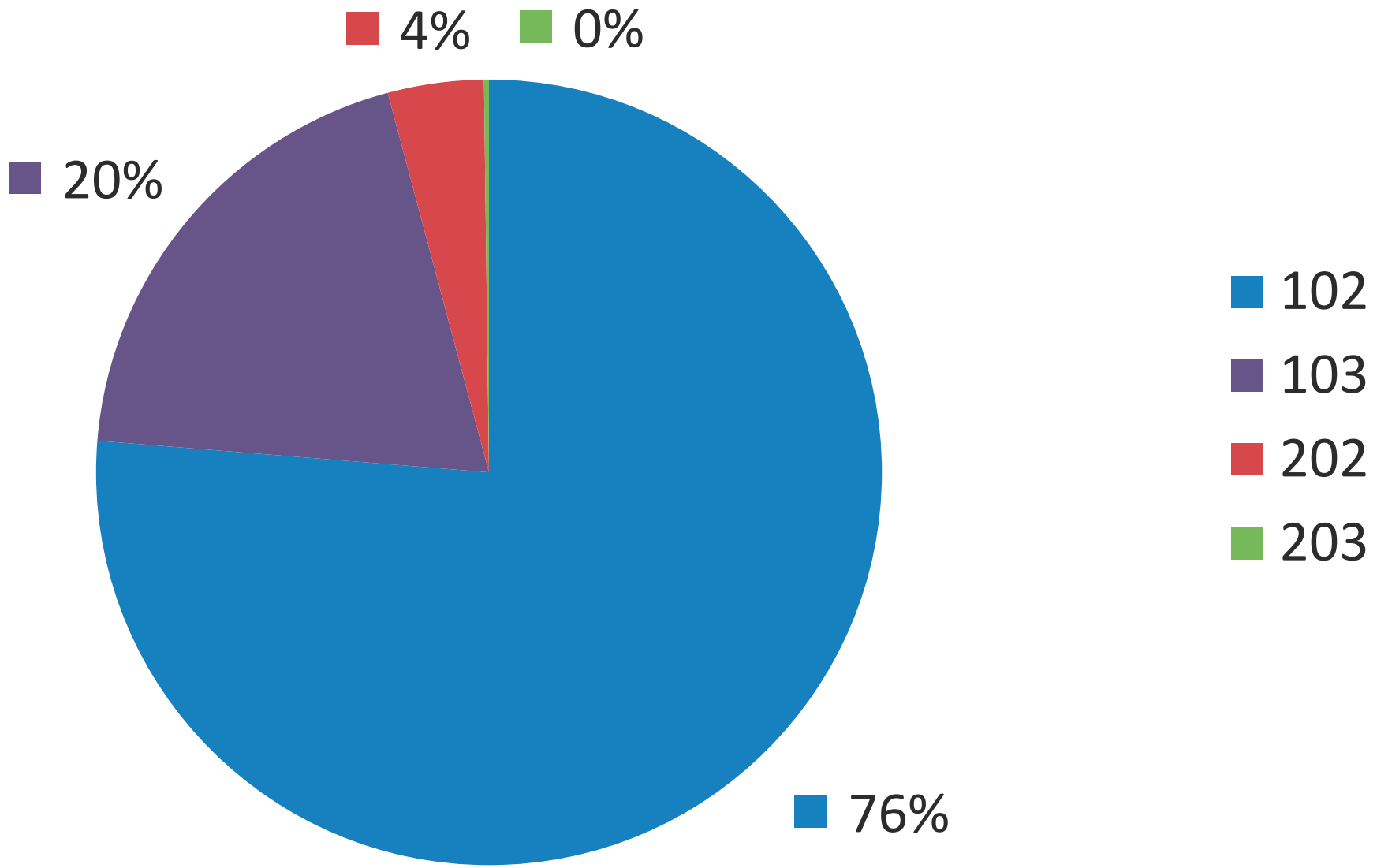
Value	*Meaning*
MFA1	City of birth
MFA2	Date of birth, formatted *MM/DD/YYYY*
MFA3	Debit card number
MFA4	Father's middle name
MFA5	Favorite color
MFA6	First pet's name
MFA7	Five digit ZIP code
MFA8	Grandmother's maiden name on your father's side
MFA9	Grandmother's maiden name on your mother's side
MFA10	Last four digits of your cell phone number
MFA11	Last four digits of your daytime phone number
MFA12	Last four digits of your home phone number
MFA13	Last four digits of your social security number
MFA14	Last four digits of your tax ID
MFA15	Month of birth of youngest sibling, *do not abbreviate*
MFA16	Mother's maiden name
MFA17	Mother's middle name
MFA18	Name of the company where you had your first job
MFA19	Name of the manufacturer of your first car
MFA20	Name of the street you grew up on
MFA21	Name of your high school football team; do not include high school name, e.g. "*Beavers*" rather than "*Central High Beavers*"
MFA22	Recent deposit or recent withdrawal amount
MFA23	Year of birth, formatted *YYYY*

OFX “MFA”

Static String

- <CLIENTUID>
  - Client generated ID
  - Checked by Server
    - TOFU
  - Static
- <AUTHTOKEN>
  - Server generated
  - Provided to client out-of-band
  - Implied static
  - *Could* be used for 2-step auth

Frequency of OFX Header: Version



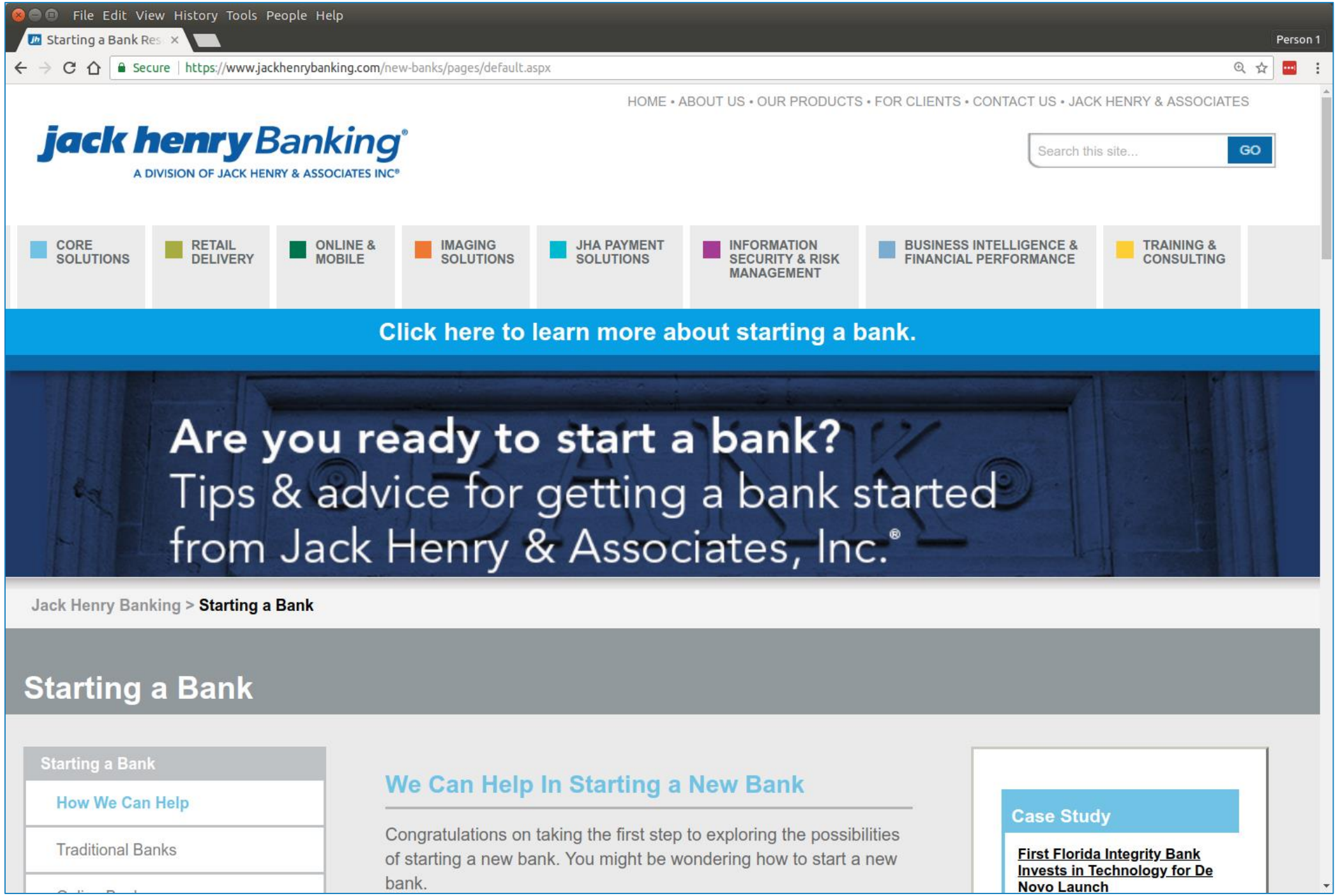
SECURITY INNOVATION

Financial Institutions

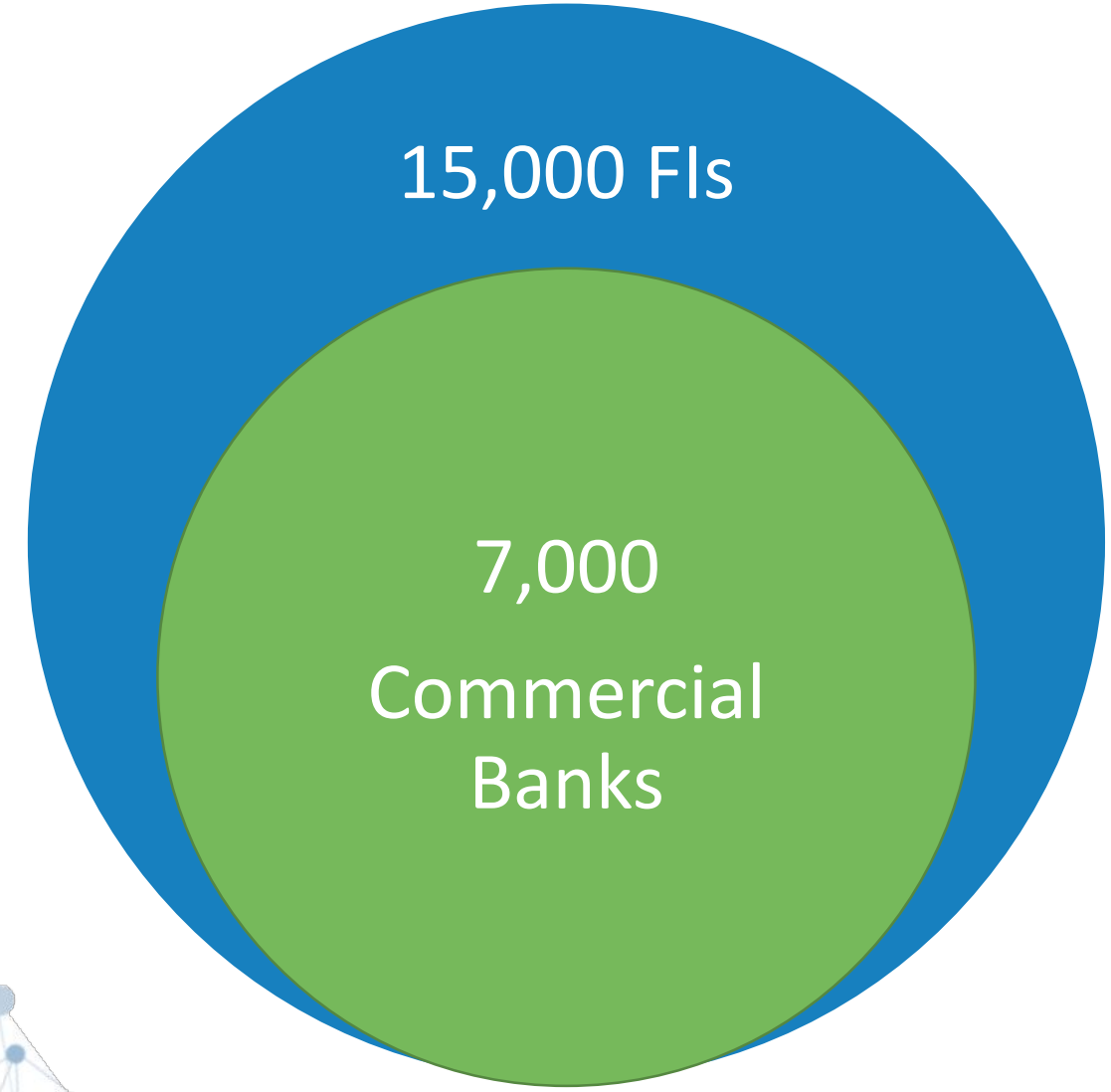
FIs

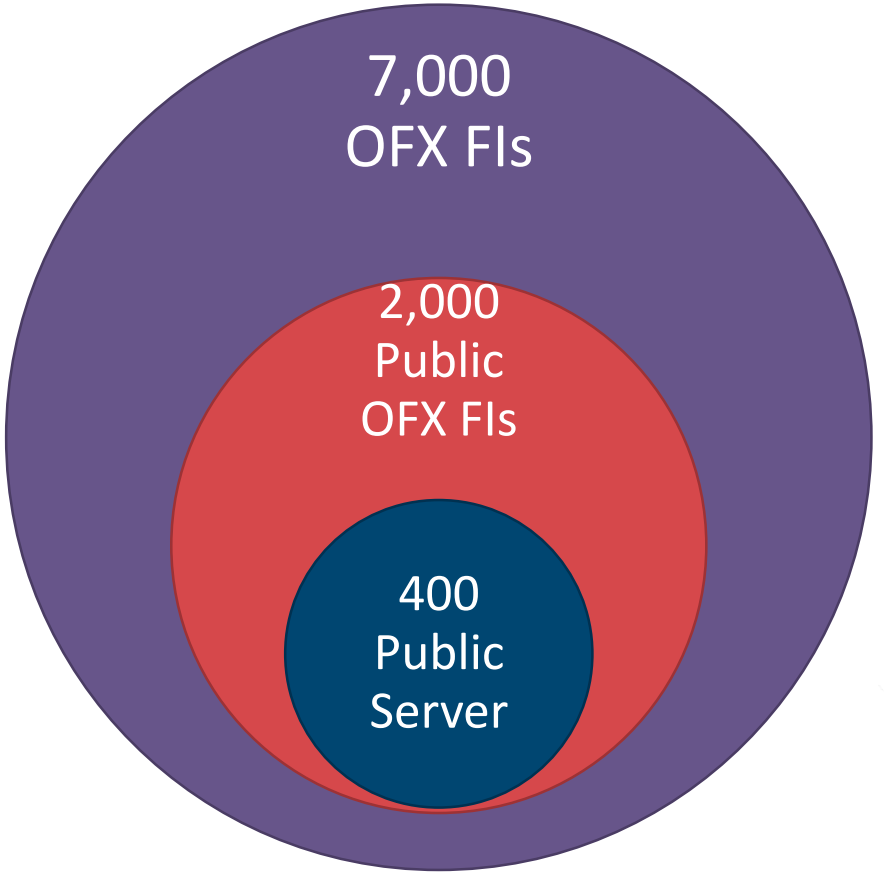
The Big Names


Yolo Federal Credit Union®
Discover the Local Difference!®
ADDITIONAL ATM LOCATED
IN LOBBY DURING
NORMAL BUSINESS HOURS
DEPOSITORY


File Edit View History Tools People Help
Starting a Bank Res
Person 1
Secure | https://www.jackhenrybanking.com/new-banks/pages/default.aspx
HOME • ABOUT US • OUR PRODUCTS • FOR CLIENTS • CONTACT US • JACK HENRY & ASSOCIATES
jack henry Banking
A DIVISION OF JACK HENRY & ASSOCIATES INC®
Search this site...
GO
CORE SOLUTIONS
RETAIL DELIVERY
ONLINE & MOBILE
IMAGING SOLUTIONS
JHA PAYMENT SOLUTIONS
INFORMATION SECURITY & RISK MANAGEMENT
BUSINESS INTELLIGENCE & FINANCIAL PERFORMANCE
TRAINING & CONSULTING
Click here to learn more about starting a bank.
Are you ready to start a bank?
Tips & advice for getting a bank started
from Jack Henry & Associates, Inc.®
Jack Henry Banking > Starting a Bank
Starting a Bank
Starting a Bank
How We Can Help
Traditional Banks
We Can Help In Starting a New Bank
Congratulations on taking the first step to exploring the possibilities of starting a new bank. You might be wondering how to start a new bank.
Case Study
First Florida Integrity Bank Invests in Technology for De Novo Launch

There Are A Lot of Banks!





(USA & Canada)

Investigation

OFX Survey

- What FI's are running an OFX server?
  - Find them and talk to them.
- What software is providing this service?
  - Ask them simple questions.

Recon

ENUM HOSTS

TLS PING

WEB SERVER

OFX SERVER

OFX PROFILE

OFX ACCOUNT

- Typical URL
  - https://ofx.bank.com/ofx/ofxsrvr.dll
- User Community
  - ofxhome.org
  - wiki.gnucash.org
- Commercial Clients
  - Branding Services
    - DNS for FIs
    - Name to OFX URL translation

Recon

ENUM HOSTS

TLS PING

WEB SERVER

OFX SERVER

OFX PROFILE

OFX ACCOUNT

- DNS
  - Stale A records?
- TLS
  - Is server certificate expired?

Stale DNS

232

Stale TLS

15

Recon

ENUM HOSTS

TLS PING

WEB SERVER

OFX SERVER

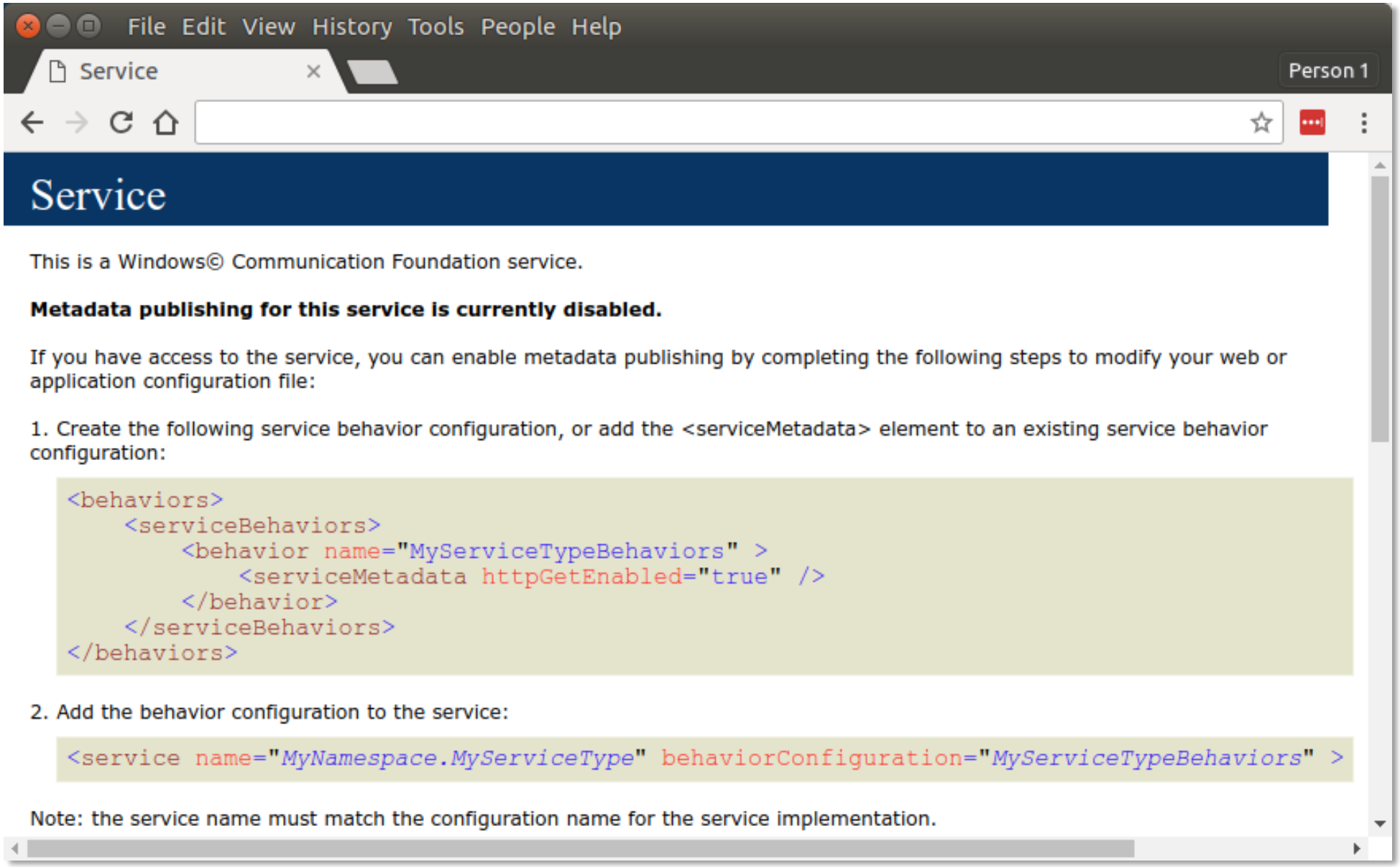
OFX PROFILE

OFX ACCOUNT

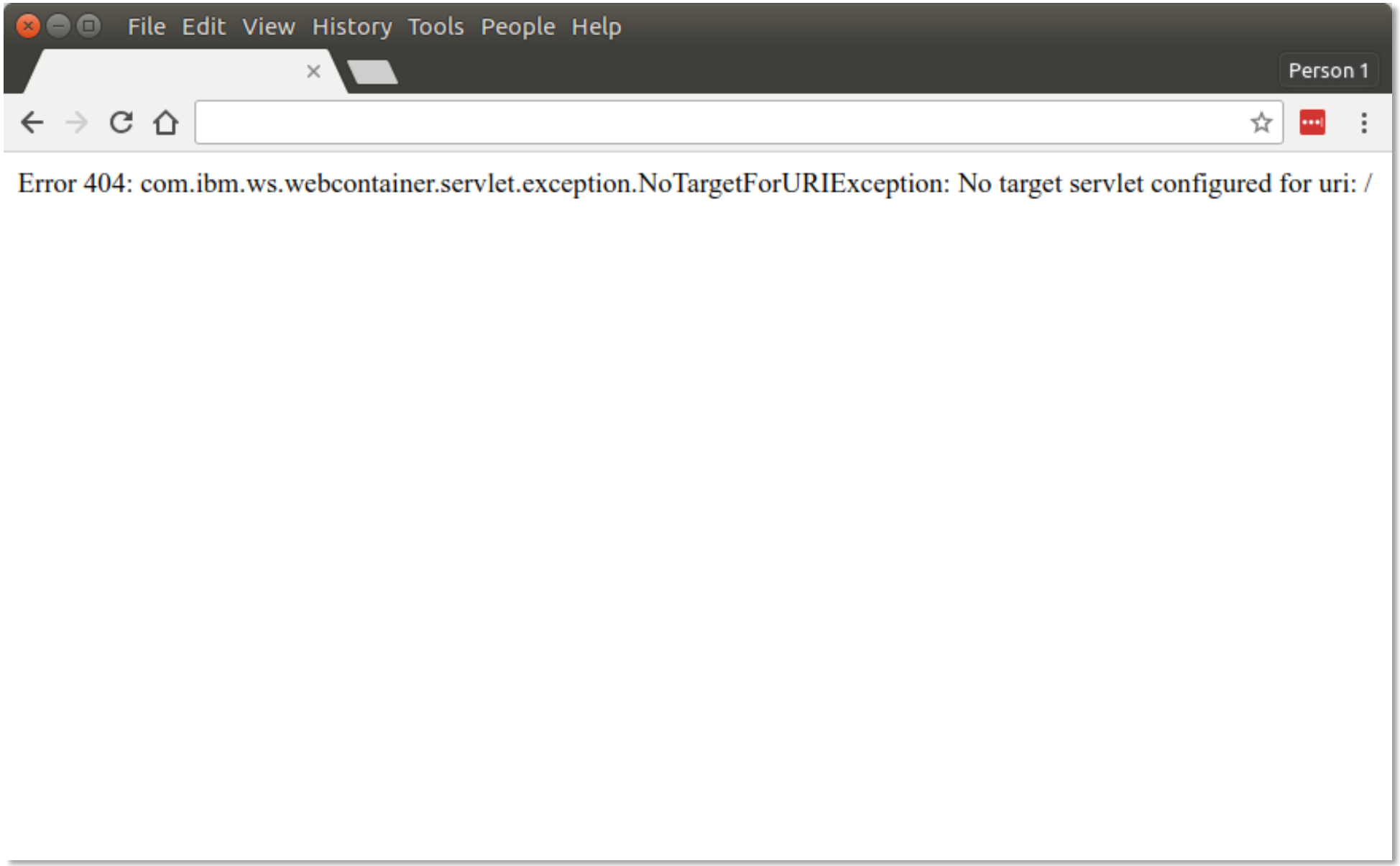
- HTTP GET /
- HTTP GET /path/ofx
- HTTP POST /path/ofx

- Fingerprint
  - Web server
  - Web application framework
  - OFX server

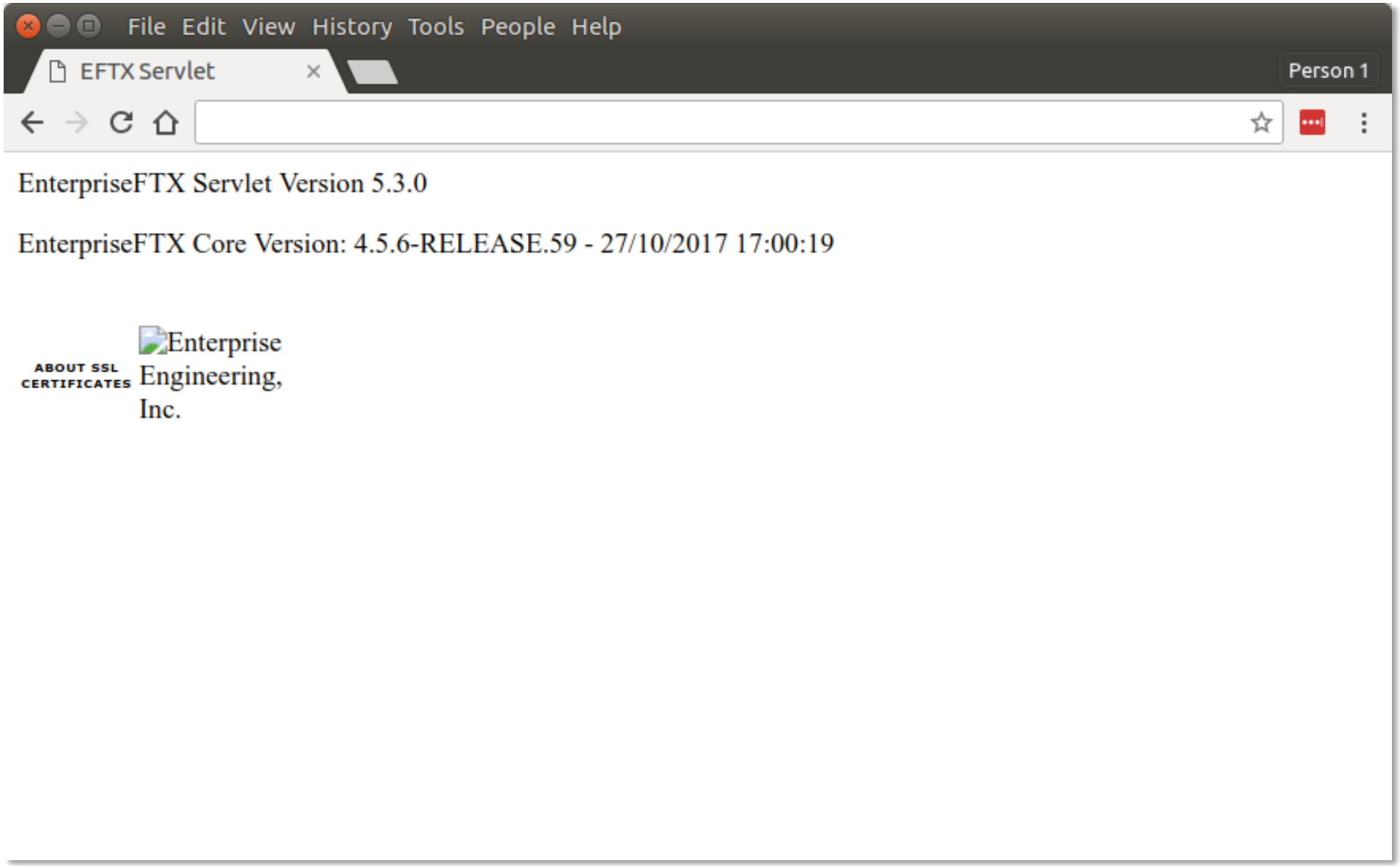
HTTP GET /


File Edit View History Tools People Help
Service
Person 1
Service
This is a Windows© Communication Foundation service.
Metadata publishing for this service is currently disabled.
If you have access to the service, you can enable metadata publishing by completing the following steps to modify your web or application configuration file:
1. Create the following service behavior configuration, or add the <serviceMetadata> element to an existing service behavior configuration:
<behaviors>
<serviceBehaviors>
<behavior name="MyServiceTypeBehaviors" >
<serviceMetadata httpGetEnabled="true" />
</behavior>
</serviceBehaviors>
</behaviors>
2. Add the behavior configuration to the service:
<service name="MyNamespace.MyServiceType" behaviorConfiguration="MyServiceTypeBehaviors" >
Note: the service name must match the configuration name for the service implementation.

HTTP GET /

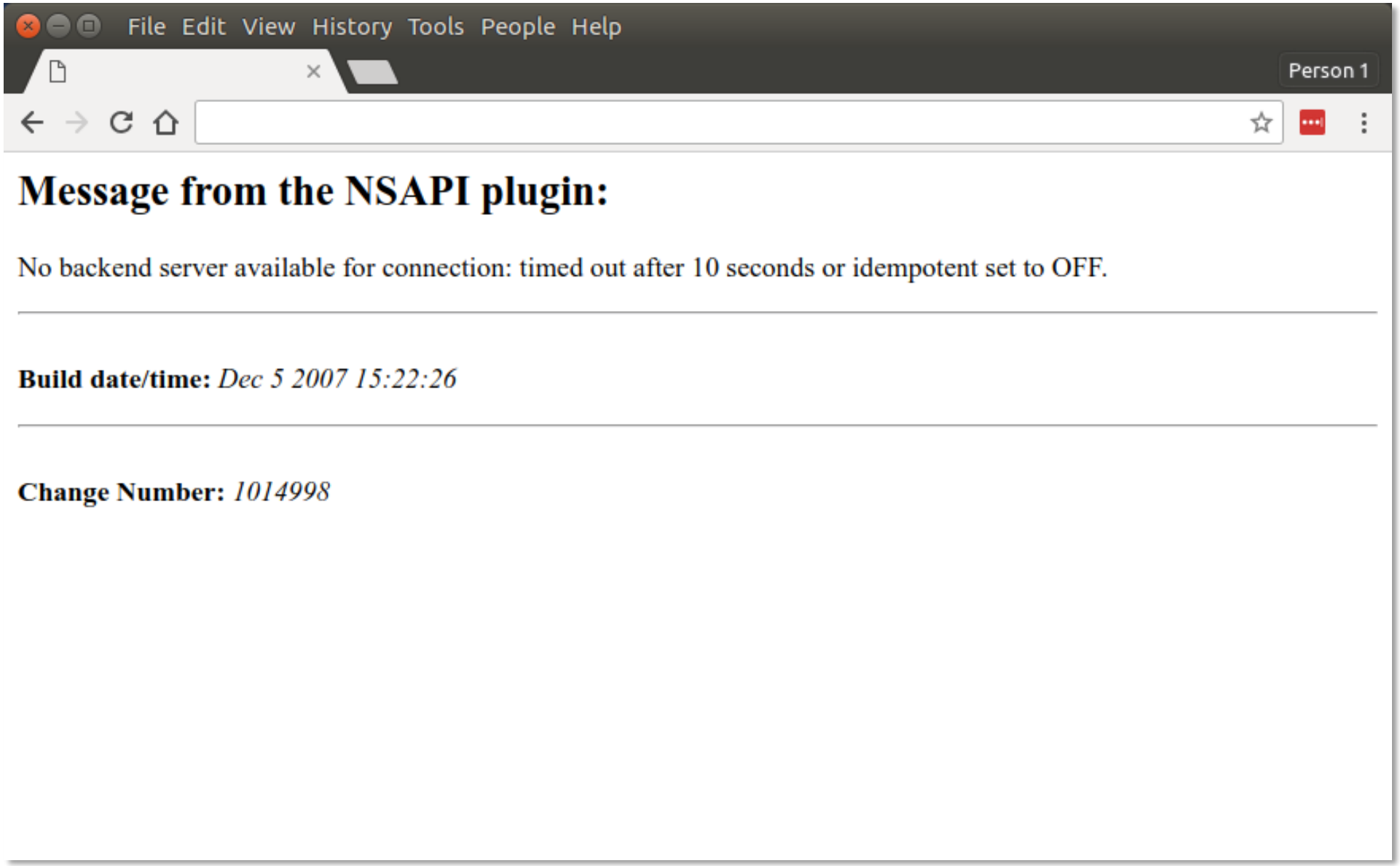

File Edit View History Tools People Help
Person 1
Error 404: com.ibm.ws.webcontainer.servlet.exception.NoTargetForURIException: No target servlet configured for uri: /

HTTP GET /path/ofx



SECURITY INNOVATION

HTTP GET /path/ofx



Recon

ENUM HOSTS

TLS PING

WEB SERVER

OFX SERVER

OFX PROFILE

OFX ACCOUNT

- HTTP POST /path/ofx
  - <OFX></OFX>
- Fingerprint
  - Framework errors
  - OFX errors

HTTP POST /path/ofx

Request

```
OFXHEADER:100
DATA:OFXSGML
VERSION:102
SECURITY:NONE
ENCODING:USASCII

<OFX>
</OFX>
```

Response

```
Error 500: java.lang.NullPointerException
```

HTTP POST /path/ofx

Request

```
OFXHEADER:100
DATA:OFXSGML
VERSION:102
SECURITY:NONE
ENCODING:USASCII

<OFX>
</OFX>
```

Response

```
OFXHEADER<OFX>
  <SIGNONMSGSRSV1>
    <SONRS>
      <STATUS>
        <CODE>2000
        <SEVERITY>ERROR
        <MESSAGE>FID  not found in file SQL State 02000
      </STATUS>
      <DTSERVER>20180324234025
      <LANGUAGE>
      <FI>
        <ORG>
      </FI>
    </SONRS>
  </SIGNONMSGSRSV1>
</OFX>
```

HTTP POST /path/ofx

Request

```
OFXHEADER:100
DATA:OFXSGML
VERSION:102
SECURITY:NONE
ENCODING:USASCII

<OFX>
</OFX>
```

Response

```
<b>Stack Trace:</b> <br><br>

<table width=100% bgcolor="#ffffcc">
  <tr><td>
    <code><pre>
[ArgumentOutOfRangeException: Length cannot be less than zero.
Parameter name: length]
   System.String.Substring(Int32 startIndex, Int32 length) +12518387
   OFX.OFX.ProcessRequest(HttpContext context) in
C:\Environment\directconnect\OFX\OFX\OFX.ashx.cs:43
System.Web.CallHandlerExecutionStep.System.Web.HttpApplication.IExecutionSt
ep.Execute() +188
   System.Web.HttpApplication.ExecuteStep(IExecutionStep step, Boolean&amp;
completedSynchronously) +69
    </pre></code>
  </td></tr>
</table>
```

Recon

ENUM HOSTS

TLS PING

WEB SERVER

OFX SERVER

OFX PROFILE

OFX ACCOUNT

- POST /path/ofx
  - <PROFRQ>
- Fingerprint
  - Spacing
  - In-house vs service provider
- Info Disclosure
  - More verbose errors
  - Long lived sessions
  - Password policy

HTTP POST /path/ofx <PROFRQ>

Request

```
OFXHEADER:100
DATA:OFXSGML
VERSION:103

<OFX>
  <SIGNONMSGSRQV1>
    <SONRQ>
      <DTCLIENT>20180319054443.123[-7:MST]
      <USERID>anonymous00000000000000000000
      <USERPASS>anonymous000000000000000000000
    </SONRQ>
  </SIGNONMSGSRQV1>
  <PROFMSGSRQV1>
    <PROFTRNRQ>
      <PROFRQ>
        <DTPROFUP>19900101
      </PROFRQ>
    </PROFTRNRQ>
  </PROFMSGSRQV1>
</OFX>
```

Response

```
OFXHEADER:100
DATA:OFXSGML
VERSION:103

<OFX>
  <SIGNONMSGSRSV1> ...
  </SIGNONMSGSRSV1>
  <PROFMSGSRSV1>
    <PROFTRNRS>
      <STATUS>
        <CODE>2000
        <SEVERITY>ERROR
        <MESSAGE>Oracle SP Adapter Error:
java.sql.SQLException: ORA-01403: no data found
ORA-06512: at “OFX_PRO.PR_GETMESSAGESETSV1",
line 54
ORA-06512: at line 1
      </STATUS>
    </PROFTRNRS>
  </PROFMSGSRSV1
</OFX>
```

HTTP POST /path/ofx <PROFRQ>

Request

```
OFXHEADER:100
DATA:OFXSGML
VERSION:103

<OFX>
  <SIGNONMSGSRQV1>
    <SONRQ>
      <DTCLIENT>20180319054443.123[-7:MST]
      <USERID>anonymous00000000000000000000
      <USERPASS>anonymous00000000000000000000
    </SONRQ>
  </SIGNONMSGSRQV1>
  <PROFMSGSRQV1>
    <PROFTRNRQ>
      <PROFRQ>
        <DTPROFUP>19900101
      </PROFRQ>
    </PROFTRNRQ>
  </PROFMSGSRQV1>
</OFX>
```

Response

```
OFXHEADER:100
DATA:OFXSGML
VERSION:103

<OFX>
  <SIGNONMSGSRSV1>
    <SONRS>
      <STATUS>
        <CODE>0
        <SEVERITY>INFO
        <MESSAGE>SUCCESS
      </STATUS>
      <DTSERVER>20180319014447.551[-4:EDT]
      <TSKEYEXPIRE>20190319120000.000[-4:EDT]
      <DTPROFUP>20081116120000.000[-5:EST]
    </SONRS>
  </SIGNONMSGSRSV1>
  <PROFMSGSRSV1>
    ...
  </PROFMSGSRSV1>
</OFX>
```

HTTP POST /path/ofx <PROFRQ>

Request

```
OFXHEADER:100
DATA:OFXSGML
VERSION:103

<OFX>
  <SIGNONMSGSRQV1>
    <SONRQ>
      <DTCLIENT>20180319054443.123[-7:MST]
      <USERID>anonymous00000000000000000000
      <USERPASS>anonymous000000000000000000000
    </SONRQ>
  </SIGNONMSGSRQV1>
  <PROFMSGSRQV1>
    <PROFTRNRQ>
      <PROFRQ>
        <DTPROFUP>19900101
      </PROFRQ>
    </PROFTRNRQ>
  </PROFMSGSRQV1>
</OFX>
```

Response

```
OFXHEADER:100
DATA:OFXSGML
VERSION:103

<OFX>
  ...
  <PROFMSGSRQV1>
  <PROFRQ>
    <SIGNONINFOLIST>
    <SIGNONINFO>
      <MIN>4
      <MAX>4
      <CHARTYPE>ALPHAORNUMERIC
      <CASESEN>N
      <SPECIAL>N
      <SPACES>N
    </SIGNONINFO>
    </SIGNONINFOLIST>
  </PROFRQ>
</PROFMSGSRQV1>>
</OFX>
```

Recon

ENUM HOSTS

TLS PING

WEB SERVER

OFX SERVER

OFX PROFILE

OFX ACCOUNT

- POST /path/ofx
  - <ACCTINFORQ>
- Fingerprint
  - Error message

HTTP POST /path/ofx <ACCTINFORQ>

Request

```
OFXHEADER:100
DATA:OFXSGML
VERSION:103

<OFX>
  <SIGNONMSGSRQV1>
    <SONRQ>
      <USERID>anonymous00000000000000000000
      <USERPASS>anonymous00000000000000000000
    </SONRQ>
  </SIGNONMSGSRQV1>
  <SIGNUPMSGSRQV1>
    <ACCTINFOTRNRQ>
      <ACCTINFORQ>
        <DTACCTUP>19900101
    </ACCTINFORQ>
  </ACCTINFOTRNRQ>
</SIGNUPMSGSRQV1></OFX>
```

HTTP POST /path/ofx <ACCTINFORQ>

Response

<MESSAGE>SUCCESS

<MESSAGE>Signon invalid

<MESSAGE>Could not process request

<MESSAGE>Unable to retrieve FI configuration.

<MESSAGE>Unsupported operation for anonymous user

<MESSAGE><FI> Missing or Invalid in <SONRQ>

<MESSAGE>There was a problem verifying the UserId/Password

<MESSAGE>Please contact your financial institution to enroll.

<MESSAGE>General error (ERROR) The server encountered an error.

<MESSAGE>Account information request could not be completed at this time. Please contact your financial institution for assistance.

<MESSAGE>Signon VALUES (for example, USER ID or Password) invalid.

<MESSAGE>User id password combination incorrect

<MESSAGE>Invalid FID sent in Request

<MESSAGE>UserID/PIN is incorrect.

<MESSAGE>No Accounts Returned

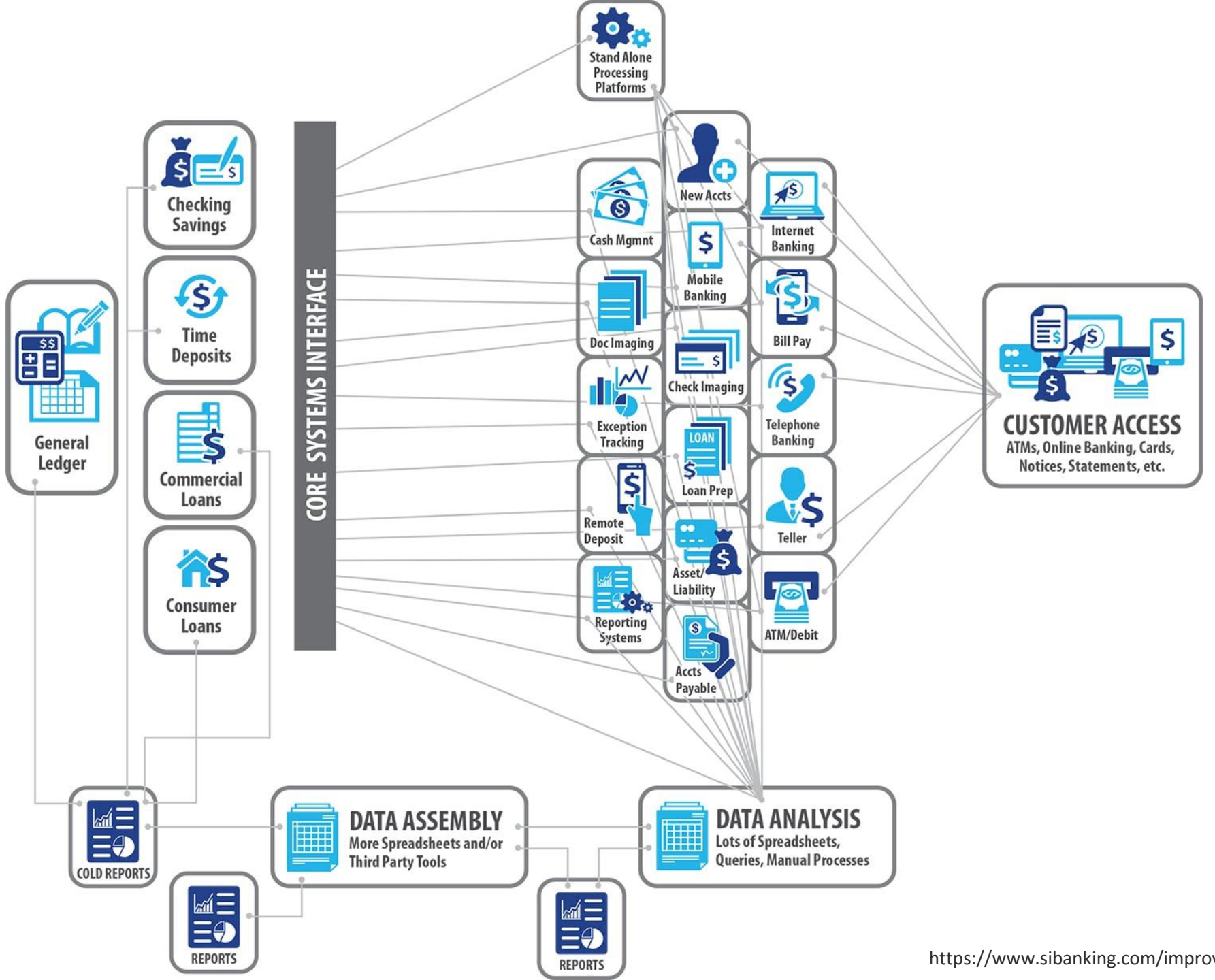
<MESSAGE>Account Not Found

<MESSAGE>Client up to date

<MESSAGE>Invalid session

<MESSAGE>General Error

Financial Software Vendors



https://www.sibanking.com/improved-core-banking-software/

Where Do I Buy?

- Not shrink wrapped
- No ‘apt install’
- No app store

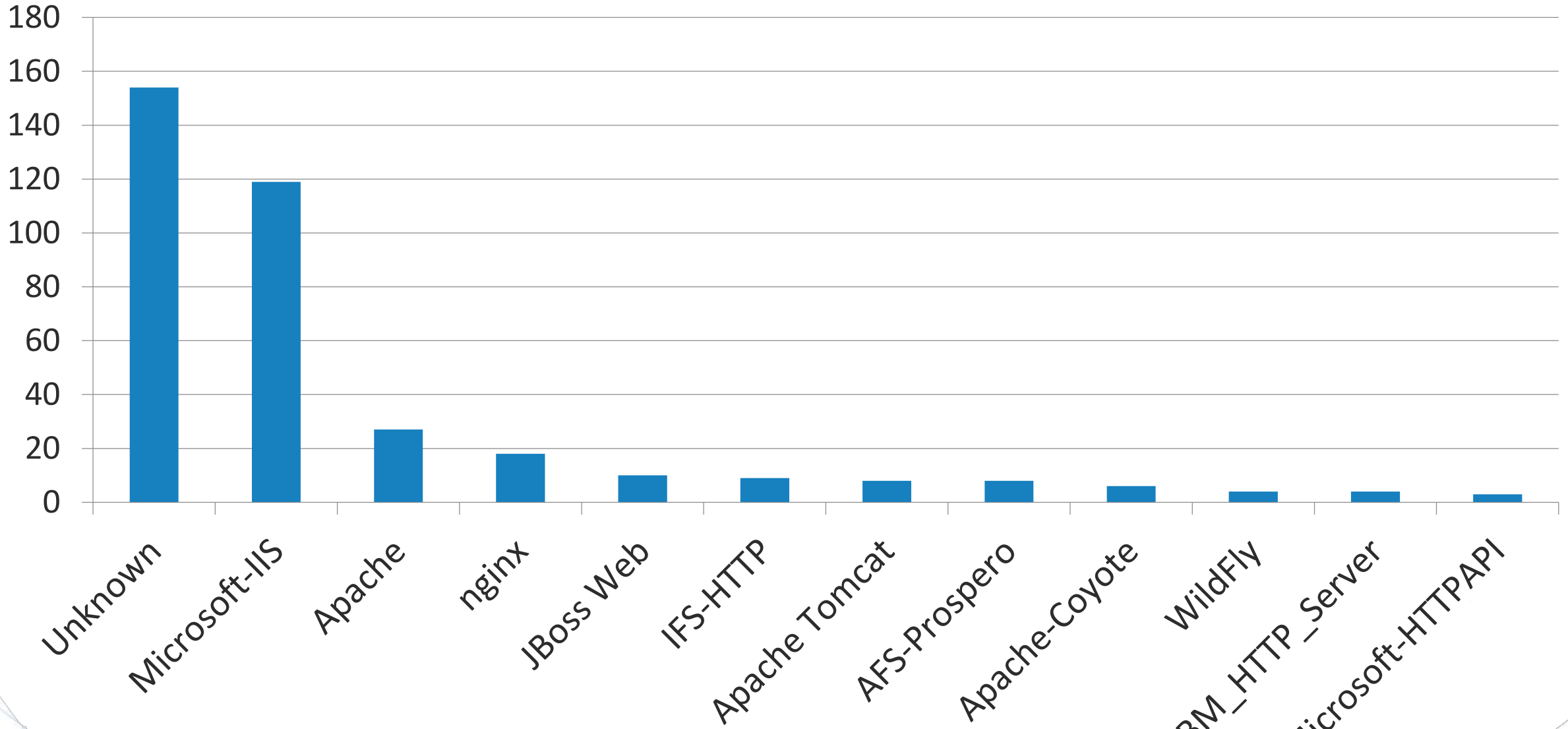
Service Providers of Financial Institution Account Connectivity

OFX Service Provider	Software Connected			Download Method		Type of Accounts that Can Download						Required Testing by Intuit *		
	Quicken Windows	Quicken Mac	Quick Books	Direct Connect	Web Connect	Banking	Credit Card	Invest-ments	401K	Pay-ments	Auto a/c setup	None*	Some Testing[1]	Full Testing[1]
Access Softek, Inc.	x	x	x	x		x					x	x		
Automated Financial Systems	x			x				x			x	x		
Automated Systems	x	x	x	x	x	x					x	x		
Cardinal Solutions	x	x	x	x	x	x	x			x				x
CheckFree	x	x	x	x		x	x			x	x			x
Corillian	x	x	x	x	x	x	x			x	x			x
Digital Insight	x	x	x	x	x	x	x			x	x	x		
DST	x	x		x	x			x			x	x		
EEI	x	x	x	x	x	x	x	x	x	x	x			x
Fidelity IFS	x	x	x		x	x							x	
Fidelity National	x			x		x				x	x			x
Financial Fusion	x	x		x		x	x			x				x
Fiserv	x	x	x	x	x	x				x	x	x		
Innovision	x	x	x	x	x	x	x	x	x		x			x
Intelidata	x	x	x	x	x	x	x			x	x			x
Jack Henry	x	x	x	x	x	x	x				x	x		
FIS/(old nameMetavante)	x	x	x	x	x	x	x	x		x	x		x	
NCR-Corillian Voyager	x	x	x	x	x	x	x			x	x	x		
Open Solutions Inc.(OSI)	x	x	x	x	x	x				x	x		x	
ORCC	x	x	x	x	x	x	x			x	x	x		
ACI Worldwide/PM Systems	x	x			x	x	x					x		
Pershing	x	x		x				x			x	x		
PSI	x	x	x	x	x	x					x			x
SciVantage	x				x			x					x	
Symitar Systems-Episys	x	x	x	x	x	x	x				x	x		

Auto-launch (without Intuit testing) is available to financial institutions whose data is hosted by the OFX Service Provider.

[1] Intuit testing fees may apply.

Frequency of HTTP Servers



Acquisition and Atrophy

https://www.fisglobal.com/about-us/about-our-company

Vulnerabilities

650 Page specification

34 Implementations

x 10 Technology Stacks

221,000 Vulnerabilities

Found in Production

- Web server disclosure
- Web framework disclosure
- OFX server version disclosure
- Backend DB disclosure
- Full stack trace on errors
- Full server file paths in errors
- Out-of-date software
- Unhandled exceptions
- Long lived session keys
- MFA ignored
- Internal IP disclosure
- Valid user enumeration
- Personal email disclosure
- Unmaintained servers
- Null values returned
- Unregistered URL referenced
- Reflected XSS
  - I know it's not a web page, and yet…

Demo

ofx-postern

- Fingerprint OFX Server
- Show capabilities
- Show disclosure vulnerabilities

https://github.com/sdann/ofx-postern

Conclusions

PLEASE
ENTER
THROUGH
SIDE
DOOR

Planning for Retirement

- **Inventory your assets**
  - How much ~~money~~ public facing services do you have?
- **Pick an age to retire**
  - How old do you want your TLS certs to be?
  - When will ~~you~~ your software stop working?
- **Do quarterly check-ins**
  - ~~Are you saving enough?~~ Is your software up to date?
- **Protect your assets**
  - With ~~insurance~~ MFA
- **Invest**
  - The earlier the better, but it is never too late to start!

Questions?

@sdanndev | www.securityinnovation.com

SECURITY INNOVATION

Glossary

- **FI** - Financial Institution
  - A bank, brokerage, or credit card provider.
- **PFM** - Personal Financial Management
  - Client software for viewing and managing their financial accounts