Your Bank's Digital Side Door

SECURITY INNOVATION

About Security Innovation

- For over **15 years**, we've helped secure software in the toughest places:

- Authors of **18 books** on security topics (10 co-authored with Microsoft)
- Over **2 million licensed users** of our training solutions (12 awards this year)
- **Gartner Magic Quadrant leader**
- Sold **SI Govt Solutions, Inc.** to Raytheon; spun off **OnBoard Security, Inc.**

BOEING · Bottomline Technologies · BROADCOM · amazon web services · intuit · RoyalCaribbean INTERNATIONAL · NIKE · SAFEWAY · sears · Coca-Cola

Honeywell · hp · htc · IBM · KRONOS · starwood Hotels and Resorts · TARGET · TSC TRACTOR SUPPLY Co · WILLIAMS-SONOMA · Carnival

SUNGARD · Symantec · TERADATA · Texas Instruments · Microsoft · AAA · Alaska AIRLINES · backcountry.com · BED BATH & BEYOND · GNC LIVE WELL

SECURITY INNOVATION

Personal Financial Management

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

Personal Financial Management (PFM)

Quicken

PERSONAL CAPITAL

intuit QuickBooks

Microsoft Money

GnuCash
Free Accounting Software

mint.com

Quicken/Quickbooks Connection Types

Web Connect

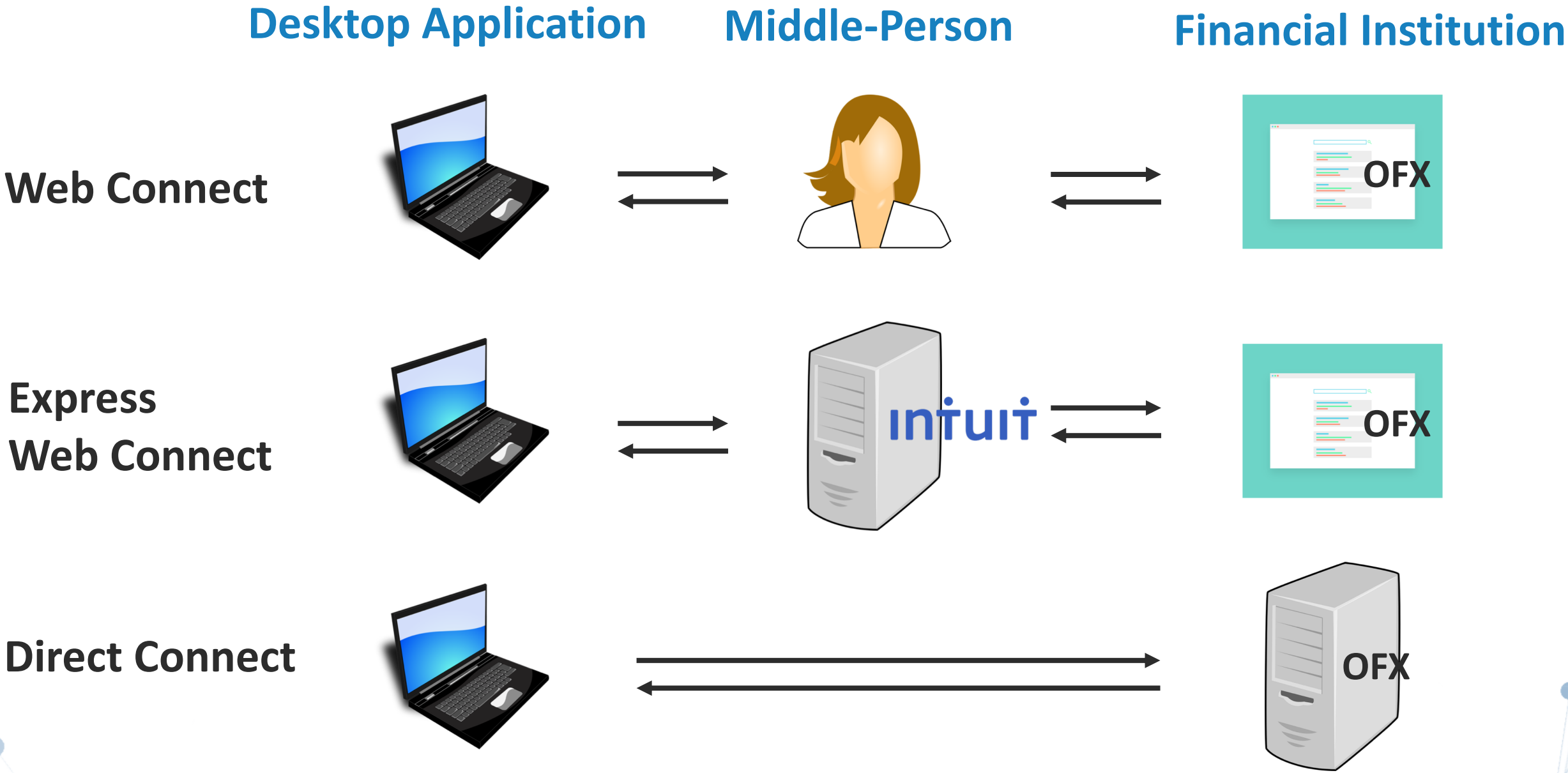
- Unidirectional
- Manual
- Download a file
- OFX file format

Express Web Connect

- Unidirectional
- Programmatic
- Screen scrape
- Private web service

Direct Connect

- Bidirectional
- Programmatic
- Structured query
- OFX protocol


Desktop Application
Middle-Person
Financial Institution
Web Connect
OFX
Express
Web Connect
intuit
OFX
Direct Connect
OFX

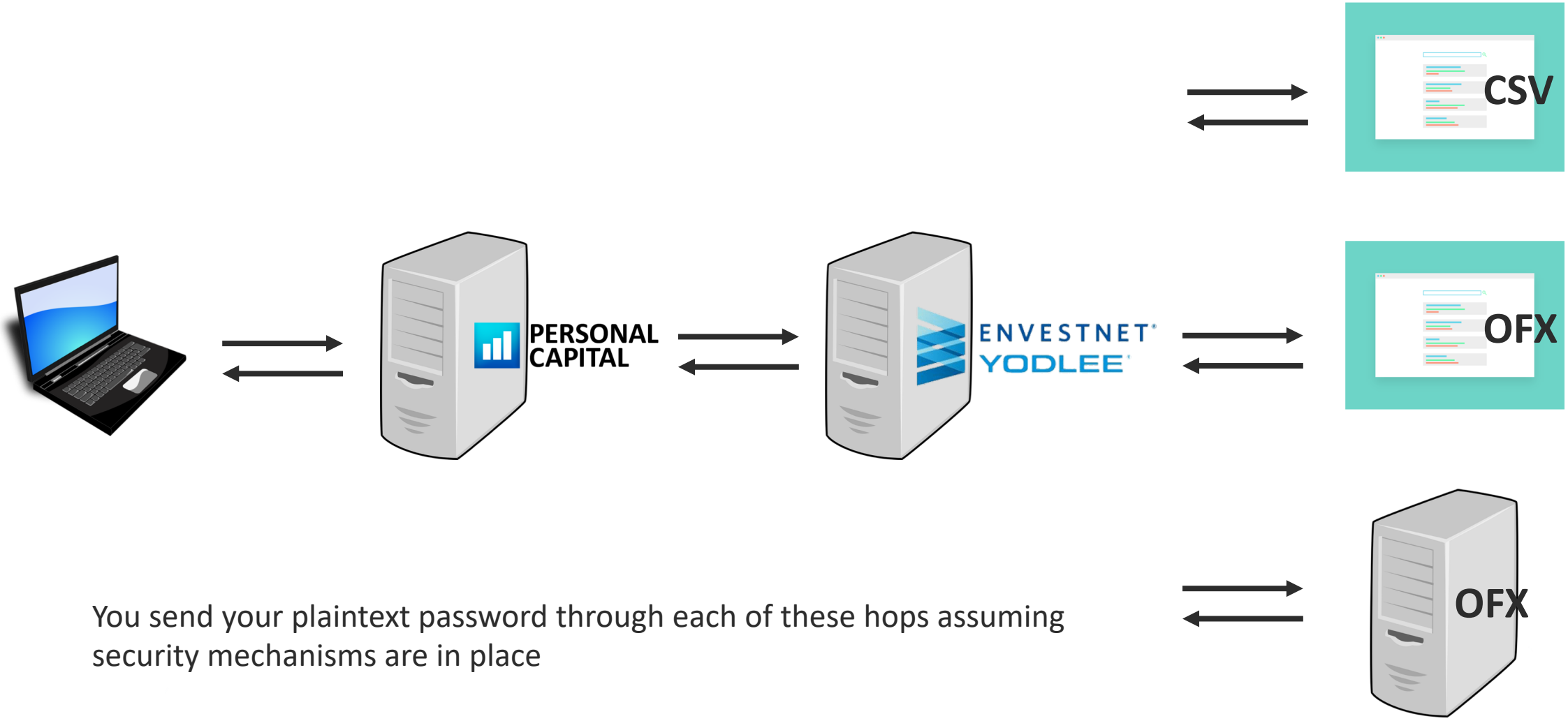
Account Aggregation Service / API

- Provide account aggregations as a service providing an API for PFM client developers
- Provide single, consistent, API across thousands of financial institutions
- Screen scraping as a service
- Also clean (normalize) the data and categorize

Web Application

Middle-“Man”

Financial Institution



You send your plaintext password through each of these hops assuming security mechanisms are in place

What Problems Does this Present?

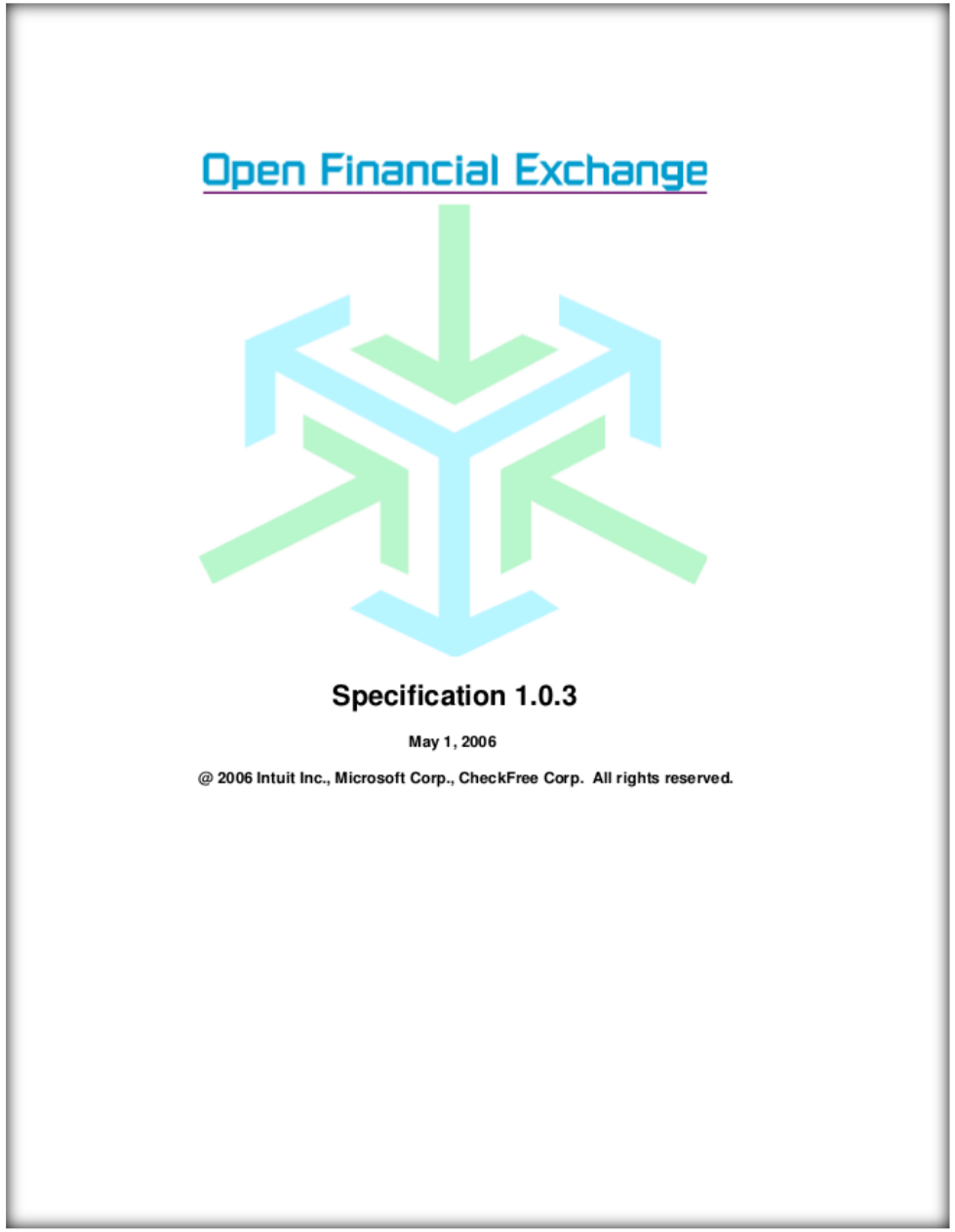
- Known vulnerabilities in OFX (protocol):
  - MFA ignored
  - SSN used as usernames
  - Internal IP, and personal email disclosure
  - Unmaintained servers
  - Unregistered URL referenced
- Bad implementation of the protocol on bank's part (similar to crypto)
- Biggest Risk: Stealing user credentials because most implementations….
  - Store and transmit credentials in plain text
  - Don't require MFA to protect against it
- Compliance
  - Most regulations state you are not compliant if you are using software with known vulnerabilities

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 (mostly) absent

Open Financial Exchange (OFX)

aka Direct Connect

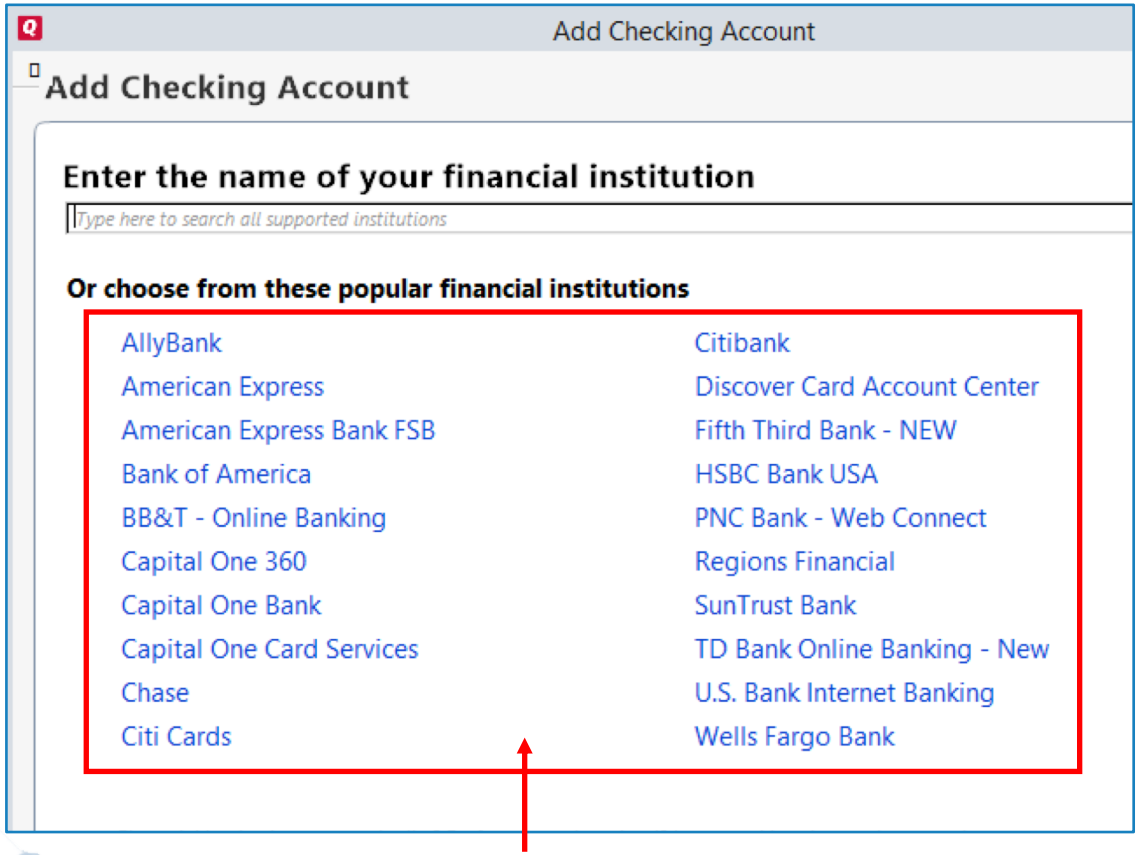

Open Financial Exchange
Specification 1.0.3
May 1, 2006
@ 2006 Intuit Inc., Microsoft Corp., CheckFree Corp. All rights reserved.

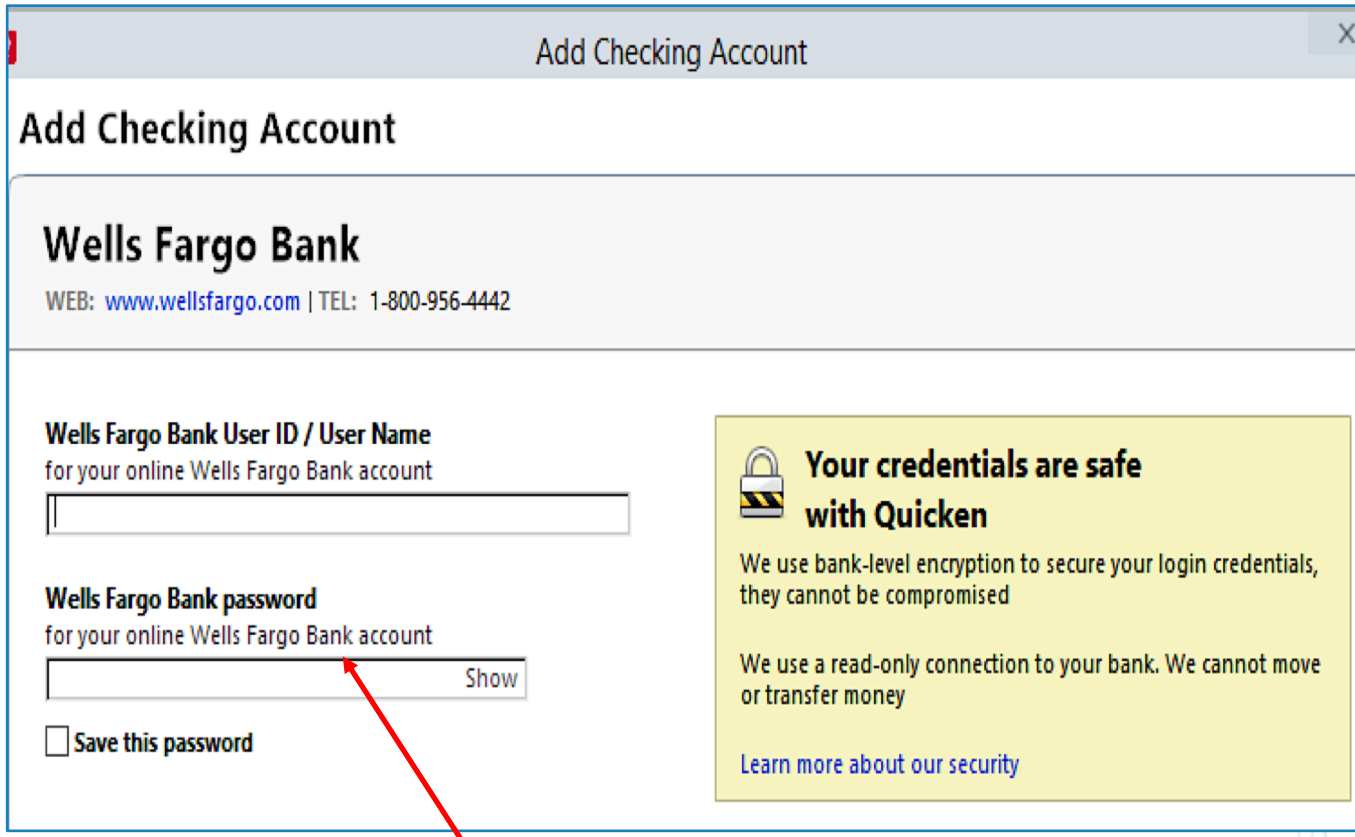
www.ofx.org

DirectConnect Offers a Wide Array of Functionality….and Hence Risk

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

The MFA Issue in Older but Popular OFX Versions





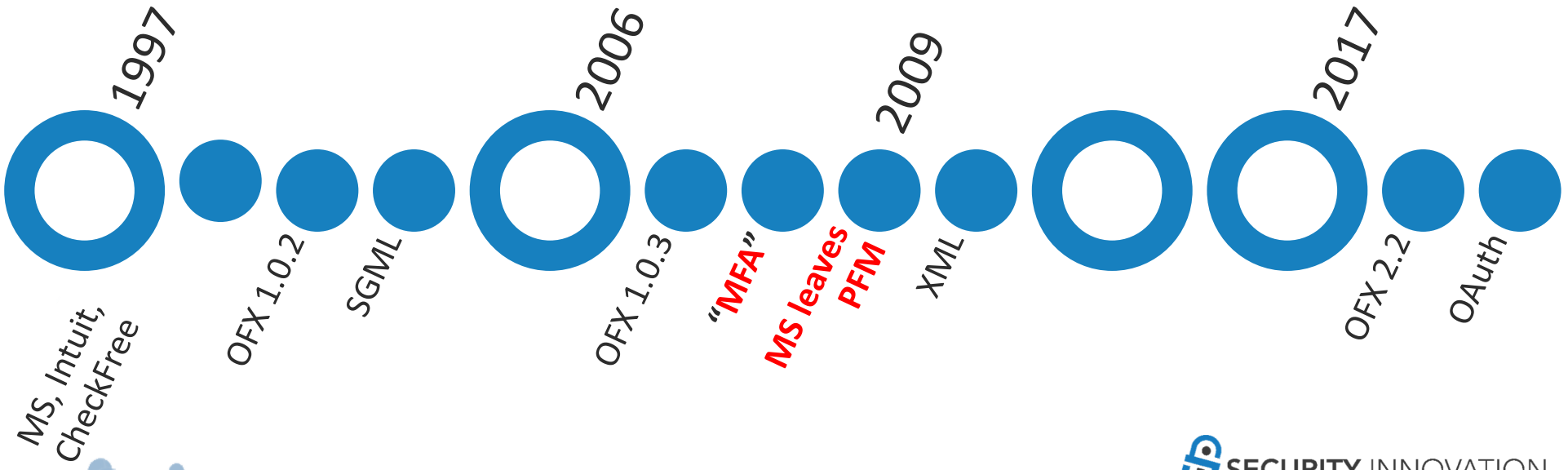
All pay to be listed and use OFX DirectConnect

Doesn't require MFA

SECURITY INNOVATION

OFX – Open Financial Exchange

- Data-stream format for exchanging financial information created by Microsoft, Intuit and CheckFree in 1997
- Allows PFM software to talk directly to a Banks OFX server
- Freely licensed; any developer can design an interface
- Many US banks and some Canadian use it



SECURITY INNOVATION

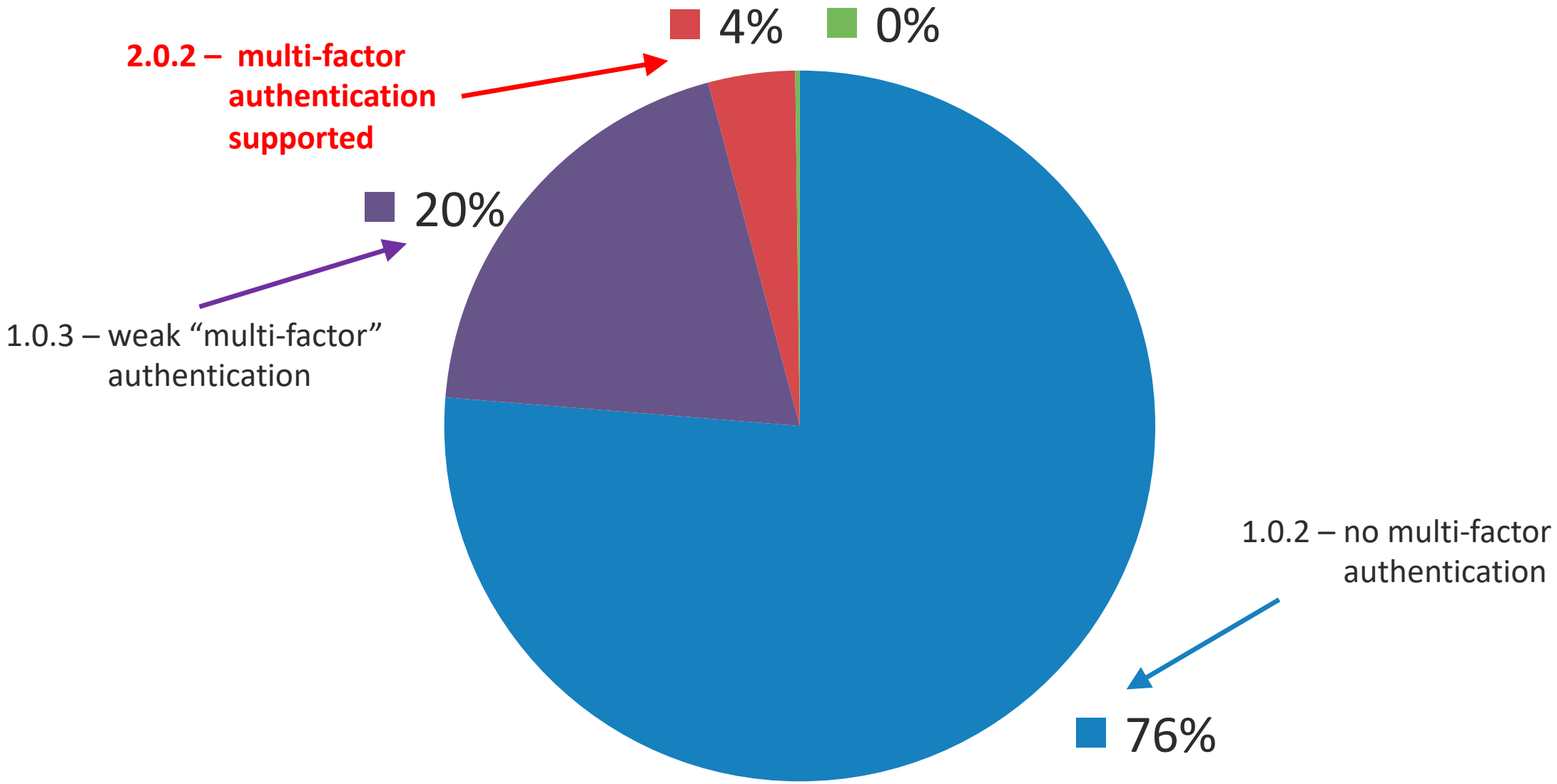
Multi-Factor Authentication (MFA)

Know	Have	Are

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

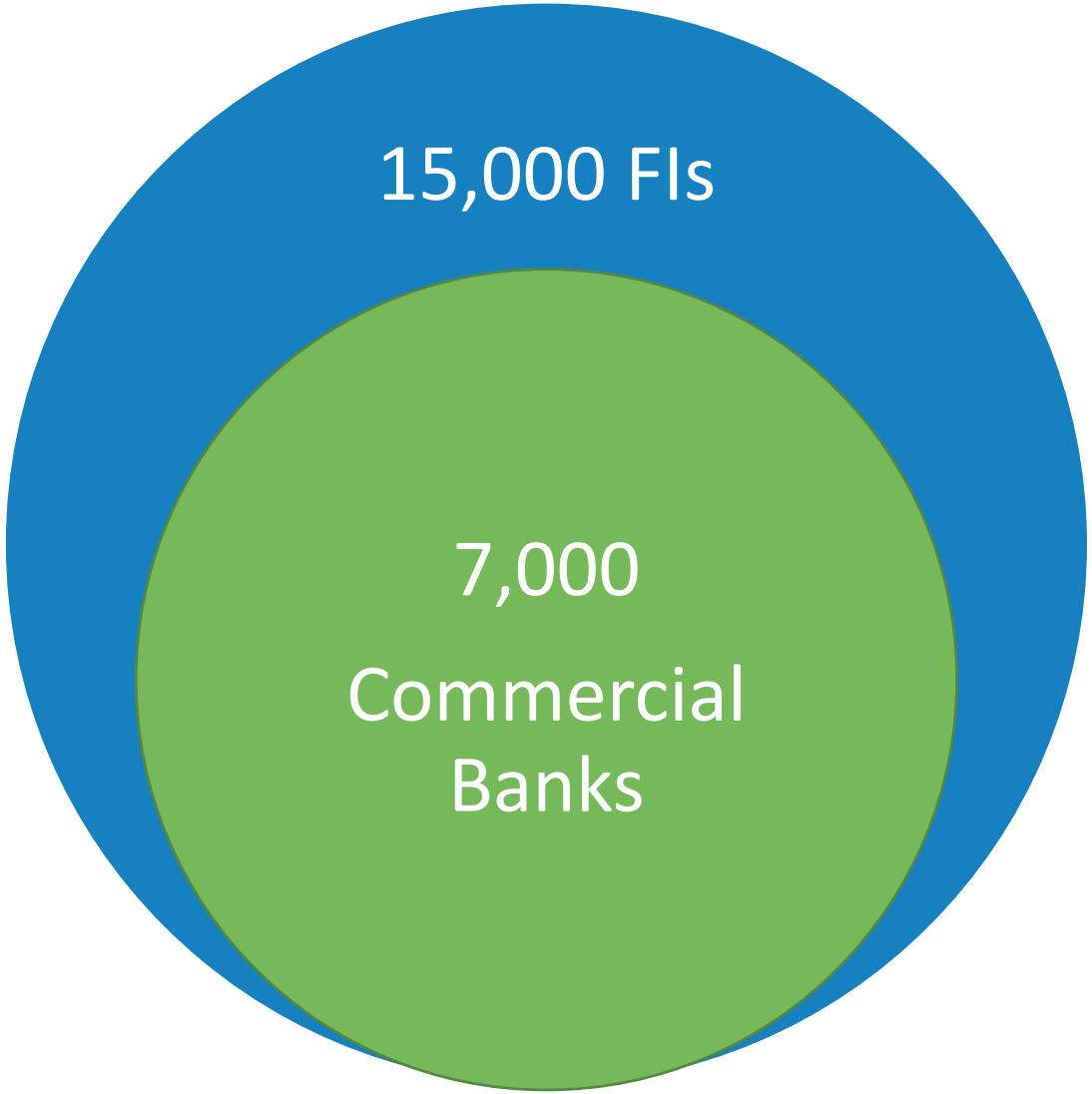
Value	*Meaning*
MFA1	City of birth
MFA2	Date of birth, formatted *MM/DD/YYYY*
MFA3	Debit card number
MFA4	Father's middle name
MFA5	Favorite color
MFA6	First pet's name
MFA7	Five digit ZIP code
MFA8	Grandmother's maiden name on your father's side
MFA9	Grandmother's maiden name on your mother's side
MFA10	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

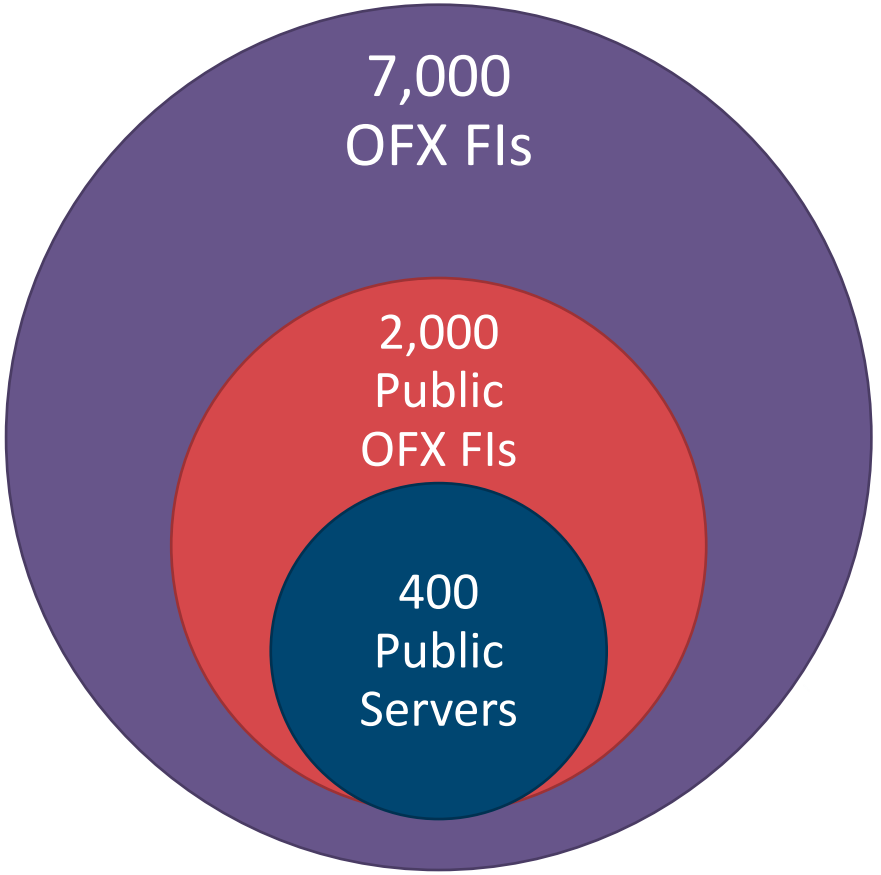
Most Banks Using OFX have Weak/No MFA



SECURITY INNOVATION

There Are A Lot of Banks!





(USA & Canada)

OFX Security/Compliance Problems 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
- SSN used as usernames
- 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…

Are the OFX security problems widespread?

- Over 3,000 North American banks support it today
- Over 30 different implementations in the wild today

What should I do?

Depends who you are, of course… ☺

- **Financial Institution**
  - Check your OFX implementation
  - Ask your Data Aggregator, OFX Provider, FinTech Vendor about
    - Their OFX implementation; require upgrade
    - Details regarding their **application security program** *(warning: they may not have one at all!)*
  - Disable, discourage, upgrade, or decrease OFX functionality
    - Web Connect only (mimic web app auth); extra fee for use; etc.
  - Robust patch/update management
    - Shalon indictment: broke into multiple FI's in 2014-2015*

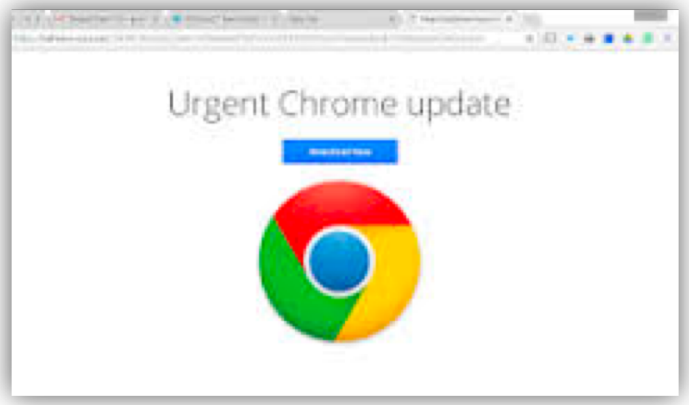
* https://www.justice.gov/usao-ndga/pr/three-charged-hacking-etrade-and-scottrade-massive-data-breach-and-identity-theft
https://www.justice.gov/usao-sdny/pr/attorney-general-and-manhattan-us-attorney-announce-charges-stemming-massive-network

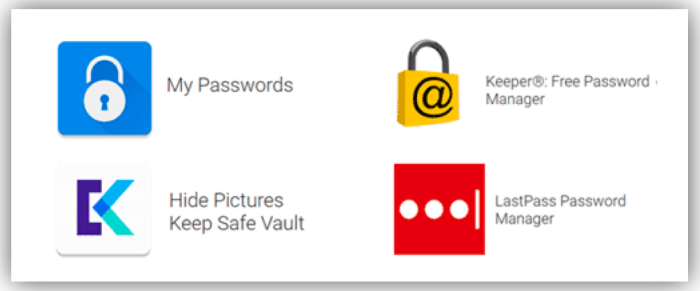
Depends who you are, of course… ☺

- **FinTech Vendor (and Aggregator, OFX Provider)**
  - Check your OFX implementation
    - Follow FDIC instructions for use of multi-factor authentication (2005)
  - **Train your development team** on secure coding
  - Conduct **robust AppSec testing** on your products
    - Vulnerability scanners alone woefully insufficient

Depends who you are, of course… ☺

- **Consumer**
  - Does your bank and PFM site use MFA or 2-step (or neither)?
  - Use a password manager (LastPass, RoboForm, Zoho)
  - Is your computer and phone updated?
    - OS, apps, browser version, A/V, et al
  - Have you conducted a personal threat model?
    - https://blog.securityinnovation.com/creating-your-own-personal-threat-model

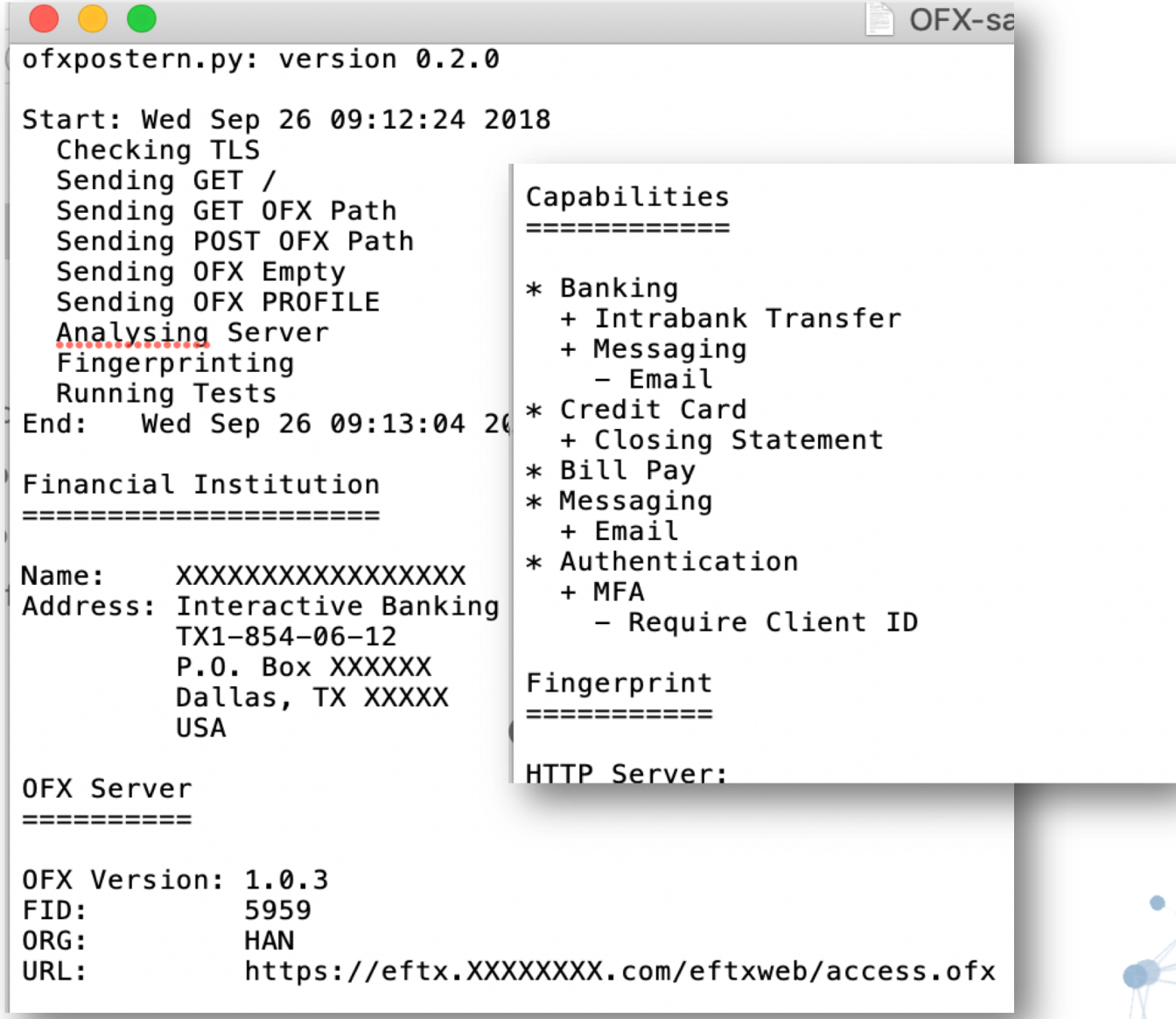




SECURITY INNOVATION

OFX Query Tool

- Freely available OSS
  - Announced at DEFCON
- Quickly assess OFX version
- List of enabled functions



https://github.com/securityinnovation/ofxpostern

SECURITY INNOVATION