NH GOVERNMENT FINANCE OFFICERS ASSOCIATION
ANNUAL CONFERENCE

May 3, 2018

What Could Possibly Go Wrong?

Bill Dwyer, NH State Treasurer

Brian Deschenes, IT Manager, NH State Treasury

What Could Possibly Go Wrong?

- Part I – "But they're our bank."
- Part II – "Ever get that feeling…?"
- Q & A

Part I – "But they're our bank."

- Who has time to monitor the financial condition of each bank we could possibly use?
- Who has time to monitor regulatory or enforcement actions taken against our bank?
- There are times when it pays to pay the experts.
- State Treasury utilizes a subscription to a monitoring/rating service for banks in NH.

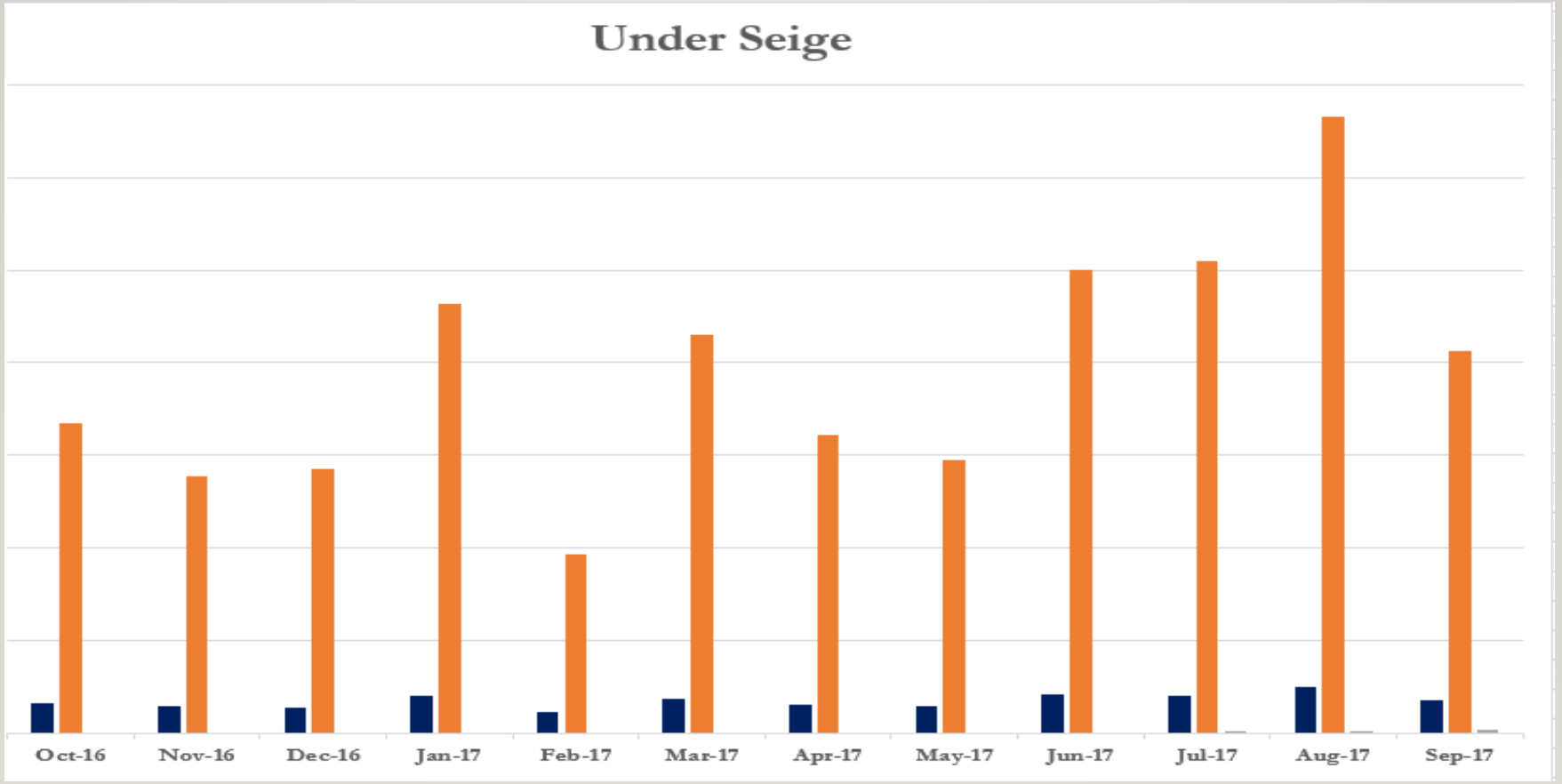
Part I – "But they're our bank."

- In the interest of objectivity, the monitoring service will not be identified or promoted here.
- However
  - If you really must know, feel free to contact your State Treasurer (email & phone on last slide).
  - In researching multiple services, a reasonable annual cost for a quarterly publication is about $200.
  - Select a service that monitors banks chartered in NH or federally chartered with a branch in NH.
- Like the credit rating agencies, each monitoring service will use its own designations.
  - Pink hearts, yellow stars, and green clovers don't matter.
  - Pay attention to how the banks are evaluated relative to one another.

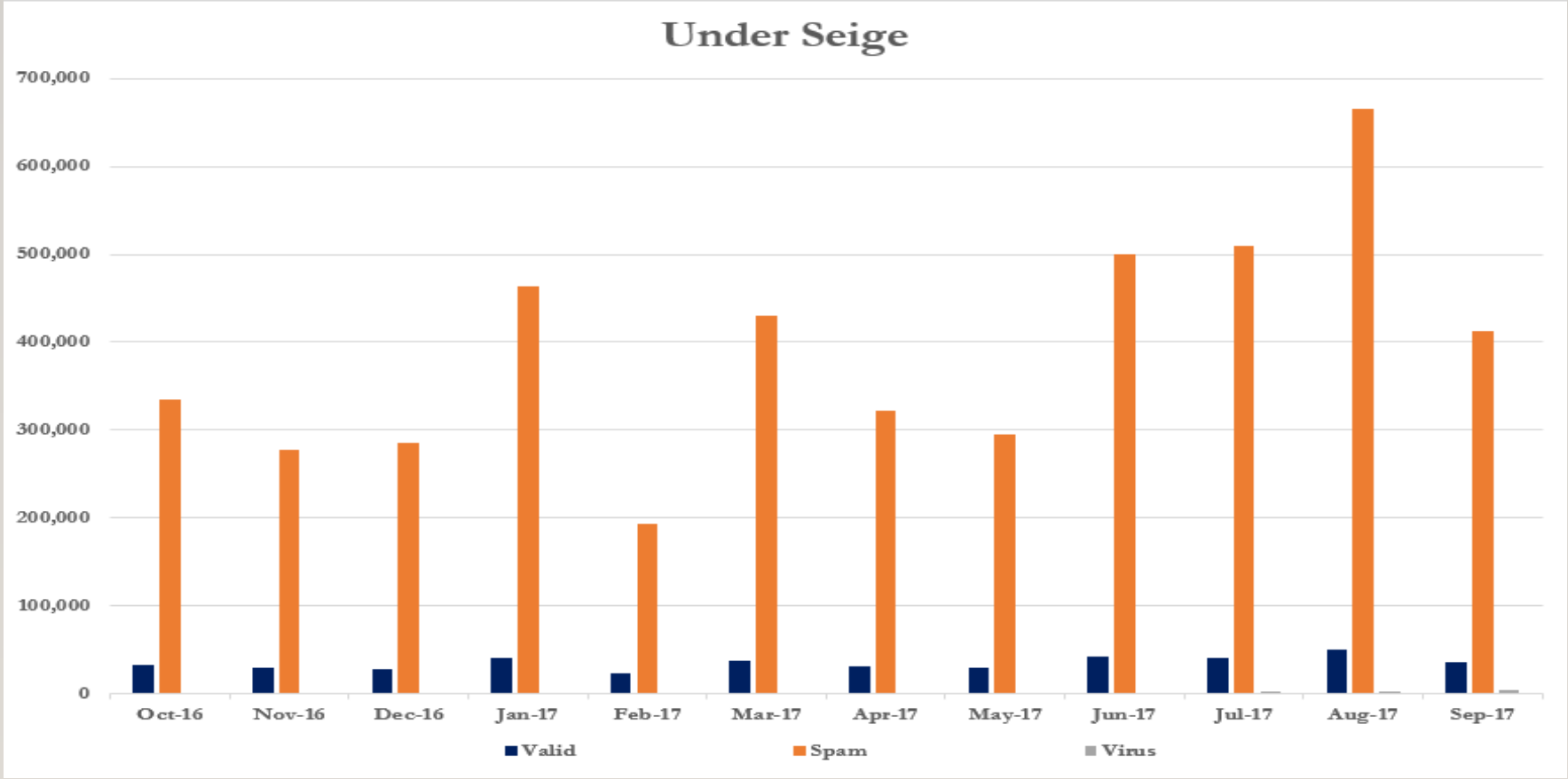
Part I – "But they're our bank."

- Use the relative ratings to decide where to deposit funds when the interest rates are similar.
- Establish a "rating" criteria below which you will not deposit funds with a bank.
  - The monitoring service should assign financial metrics to each designation it uses.
  - Whenever you have concerns or reservations, express them to your banker.
- Enforcement actions are important and can inform your decisions, however…
  - It seems that at one time or another, some large federally-chartered banks run afoul of regulators.
  - If you decide to pick one fight, be prepared to pick them all (Wells Fargo example).
  - The severity of any violation is in the eye of the beholder, so be consistent and objective.

Part II – "Ever get that feeling..."



Part II – "Ever get that feeling..."



Part II – "Ever get that feeling..."

- **Email Spoofing** - the creation of email messages with a "forged" sender address.
- **Email Phishing** - a form of social engineering that uses email to trick the user into disclosing sensitive info (i.e., login credentials, account numbers, or other confidential data).
- **Spear Phishing/Whaling** - similar to phishing but a more targeted form of social engineering directed at an individual, organization, or business; similar to Spear Phishing, Whaling attempts stalk the "bigger fish" (i.e., executives, politicians, or high-profile individuals).

Part II – "Ever get that feeling..."

- In 2017 alone, damaging phishing attacks demonstrated that anyone can fall victim to this type of fraud tactic.
  - March 17th, 2017 – 205 Organizations reported successful Phishing attacks targeting W-2 records, subjecting more than 120,000 taxpayers to identity fraud/theft[1].
  - April 27th 2017 – Google and Facebook were out over $100 million when an attacker used a Phishing email to trick employees into wiring money to the fraudster over a two year span[2].

Sources: [1] https://www.databreaches.net/victim-of-w-2-scams-2017-list/
[2] http://fortune.com/2017/04/27/facebook-google-rimasauskas/

Part II – "Ever get that feeling..."

- Be vigilant when it comes to email – It's always better to err on the side of caution and assume that if it doesn't look right, it probably isn't (poor grammar was a classic giveaway).

- Not sure if it's Phishing? Call the Person/Coworker or Company directly to confirm the communication (don't use the contact info in the questionable email).

- Make sure you are running the latest and up-to-date versions of your Internet Browser, Operating System, Office applications and Endpoint Security Software (set automatic updating for all your software).

Part II – "Ever get that feeling..."

- Vendor/Supplier and Procurement Fraud – Be mindful of scams to divert payments to cybercriminals.
  - Emails requesting bank account changes for particular vendors you conduct business with.
  - Urgent Phone calls from someone asking to change electronic payment instructions or the mailing address for checks.
  - Fake invoices through email, fax, or mailed directly to your office.

Part II – "Ever get that feeling..."

- User and Administration of Financial Partners' Online Systems.
  - Dual controls of online banking administration.
  - Reduced function online banking administrators – Banks typically default system administrators to possess all functional accesses within online banking applications.
  - In a multi-user online banking environment, account signers should avoid serving as banking system administrators.
  - Consider pushing user administration back to the bank, particularly if staffing resources are limited.
  - All of these measures reduce exposure to internal fraud risk.

Part II – "Ever get that feeling..."

- Cybersecurity Awareness Training & Culture – Continuous reminders of the everyday threats, minimum annual training, sharing stories, etc.
- Risk Assessments – Perform annual risk assessments to identify weaknesses and reduce risk. Review of 3rd party SSAE18/SOC Reports.
- Penetration Testing - Include social engineering tactics (test the "human firewall").
- Information Classification Matrix - Identify where your sensitive data resides, then organize and classify the information based on regulation and compliance.

What Could Possibly Go Wrong?

Bill Dwyer

NH State Treasurer

(603) 271-2624

bdwyer@treasury.state.nh.us

Brian Deschenes

NH State Treasury IT Manager

(603) 271-8413

bdeschenes@treasury.state.nh.us