October 2021 | Vol. 13 | Issue 1

THE QUARTER

Newsletter of the PA Department of Banking and Securities

Not If, But When:
Maintaining Cybersecurity Vigilance

FinCEN Ransomware Trends Analysis

Beware of Student Loan Forgiveness Scams

Updated Online Cybersecurity Guide

pennsylvania
DEPARTMENT OF BANKING
AND SECURITIES

IN THIS ISSUE

Stay informed!
Subscribe to *The Quarter*

SUBSCRIBE

SECRETARY

dobssecretary@pa.gov

Richard Vague

Not If, But When: Maintaining Cybersecurity Vigilance

October is National Cybersecurity Awareness Month and offers a timely reminder to take a close look at our habits and evaluate our potential risk. Each individual and business should take a critical look at ourselves to determine how we can remain prepared for a cyberattack. Unfortunately, it is no longer a matter of *if* when it comes to data breaches, ransomware attacks, or other malicious cyber events, it is a matter of *when*.

Data security is an ongoing, persistent risk for nearly every industry. This is especially true for the banking industry. Banks are a target for cybercriminals by virtue of the sensitive, high value data they collect, including Personally Identifiable Information (PII), wire transfer capabilities, and other financial information. This valuable data makes financial institutions prime targets for phishing threats, persistent ransomware attacks, and other malicious threats.

The average annual loss for U.S. banks calculated on an industrywide basis is $213 million according to a recent Fitch Ratings report. According to a new FinCEN trend analysis, $590 million worth of ransomware payments were made during the first six months of 2021.

According to the 2021 Norton Cyber Safety Report, more than 475 million consumers from 10 countries have been the victim of a cybercrime, with nearly 330 million in the past 12 months alone.

The attacks appear to be becoming even more brazen and large-scale. In May 2021, we have seen one of America's largest pipelines taken offline following a ransomware attack, causing U.S. gas prices to soar and costing the company $4.4 million in cryptocurrency paid in ransom. Though later the U.S. Department of Justice was able to recover a little more than half of the payment. Just this month, one of the largest television station operators in the country, Sinclair Broadcast Group, fell victim to a ransomware attack and is still assessing the impact to its business. And those are just two examples.

There are resources available to assist you in your cybersecurity preparedness.

Consumers looking for ways to better protect themselves and their families can start with the commonwealth's online Protecting Yourself Online cybersecurity guide and can explore the department's events related to cybersecurity. The department also provides a number of cybersecurity updates, alerts, and links to resources focused on businesses.

I ask you to evaluate (and revisit often) your personal and business habits as they relate to cybersecurity and use of technology and encourage you to avail yourself of the resources provided by the department and other agencies.

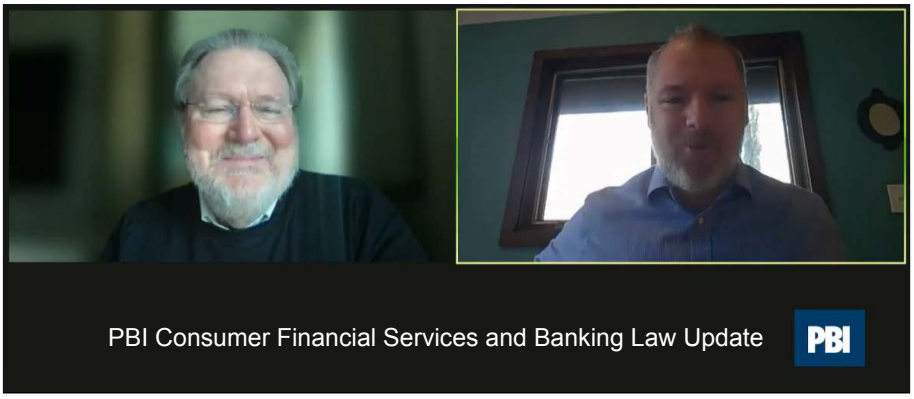
2022 CSBS Community Bank Case Study Competition Open

The Conference of State Bank Supervisors (CSBS) Community Bank Case Study Competition for 2022 is now open. Pennsylvania college and university faculty and students are encouraged to enter this year's national contest.

This competition encourages undergraduate college students to explore community banking by partnering student teams under the guidance of a faculty member with local banks to conduct original case studies. Last year, more than 50 teams participated, including 16 teams representing 13 Pennsylvania colleges and universities.

The topic for this year's competition will ask participants to look back over the last 10 years to identify the most significant developments for the community bank and look forward to predict the most significant changes to expect in the next 10 years. The full 2022 topic will be released in November.

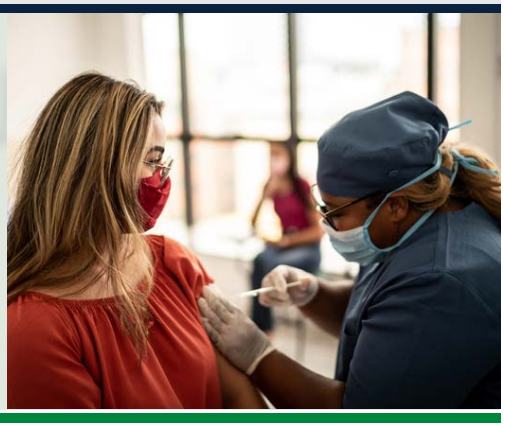
Faculty advisors can submit their statements of interest until January 10, 2022 at www.csbs.org/bankcasestudy.



Secretary Vague, joined by moderator Jason M. Cover, addressed participants during the virtual PBI Consumer Financial Services and Banking Law Update on October 21.

Secretary Vague spoke with Mid Penn Bank board members and executives during a meeting on October 26 in Hershey.

Banking on the COVID-19 Vaccine



President and CEO of the Pennsylvania Association of Community Bankers Kevin Shivers and Secretary Vague are urging their fellow Pennsylvanians to get the COVID-19 vaccine. According to data from the CDC, as of Oct. 25, 71.4% of Pennsylvanians age 18 and older are fully vaccinated. Citing the importance of keeping ourselves and our communities healthy and safe, they point to data showing that vaccines slow the transmission of the virus. Read more in their co-authored essay appearing in the Erie Times – News.

2022 Bank Holidays

Here is a list of 2022 legal bank holidays as extracted from Section 113 of the Banking Code of 1965, as amended.

When a fixed holiday falls on a Sunday, it shall be observed on the following Monday; when it falls on a Saturday, it may also be observed on the following Monday.

Fixed Holidays

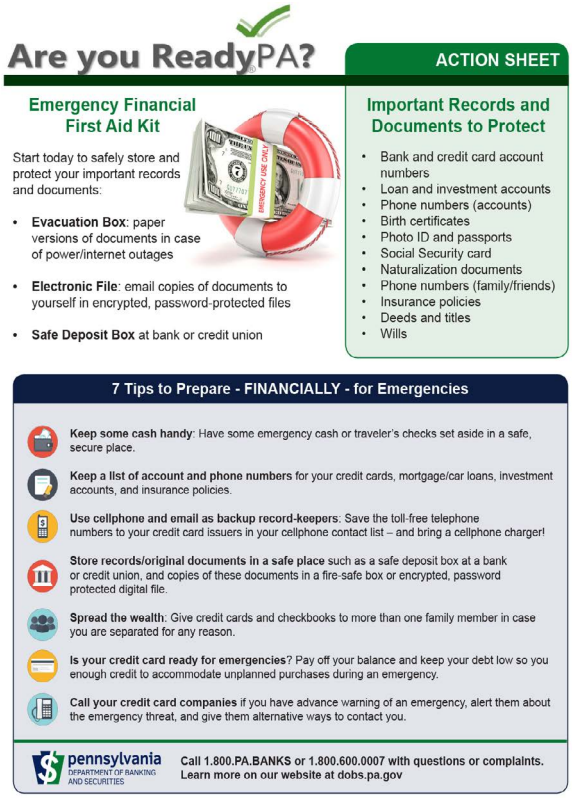
January 1 – New Year's Day
January 17 – Dr. Martin Luther King, Jr. Day
May 30 – Memorial Day
June 19 – Juneteenth
July 4 – Independence Day
September 5 – Labor Day
November 24 – Thanksgiving Day
December 25 – Christmas Day

Optional Holidays

February 12 – Lincoln's Birthday
February 21 – Washington's Birthday
April 15 – Good Friday
June 14 – Flag Day
October 10 – Columbus Day
November 8 – Election Day
November 11 – Veterans' Day

Emergency Financial Preparedness

It's always the right time to plan for a potential emergency. Use this tip sheet as a guide to getting your important documents, records, and information organized should you face an emergency.



The PA School Boards Assoc. (PSBA) hosted a PSERS panel discussion on October 13 with (from l to r) PA Treasurer Stacy Garrity, Secretary Vague, and PSBA CEO Nathan Mains.

Don't Be Wooed by Online Romance Scams

Online scams aimed at taking advantage of people on dating apps and other social media sites are on the rise. According to the FBI, the Internet Crime Complaint Center (IC3) received more than 1,800 complaints related to these online romance scams from January 1 to July 31 this year. The resulting loss was approximately $133 million.

A recent report by the Federal Trade Commission (FTC), older adults reported the highest aggregate dollar loss to romance scams in 2020.

Anatomy of an Online RomanceScam:

The scammer may:

- Make contact through dating apps or social media
- Gain victim's confidence and trust, usually through the promise of shared affection or illusion of romantic relationship
- Ask the victim fr money or even cryptocurrency investment under the pretense of an emergency or other unexpected need
- Stop communication with the victim abruptly

Protect Yourself:

- Never send money or invest based on the advice of someone you only know online.
- Do not share your financial or personal information.
- Beware of anyone who urges you to act fast on a financial opportunity that promises hard-to-believe returns.
- Search online for the person, their job, or similar stories to theirs to find information on common scams.
- Reverse image search their profile photo to see if it is associated from any other names.

If you think you have been the victim of a romance scam, report it to the FTC at ReportFraud.ftc.gov or IC3 at ic3.gov/Home/FileComplaint.

OUTREACH Spotlight

Upcoming Events

Upcoming Consumer Events

Cybersecurity – Tips for Holiday Shopping

Pathways Institute
November 1: 10:00 AM to 11:00 AM
November 9: 10:00 AM to 11:00 AM

Cybersecurity – Keeping Yourself Safe Online

Cleve J. Fredricksen Library (Virtual)
November 9: 6:00 PM to 7:00 PM
November 16: 11:00 AM to 12:00 PM

Avoiding Scams and ID Theft

Heidelberg Area Retired Persons (HARP)
November 2: 11:00 AM to 12:00 PM

Ephrata Public Library (Virtual)
November 16: 7:00 PM to 8:00 PM

Budgeting for Your New Year's Goals
Malvern Public Library (Virtual)
November 2: 7:00 PM to 8:00 PM

Fraud BINGO

Bosler Memorial Library (Virtual)
November 3: 7:00 PM to 8:00 PM

Investing in Women

Women's Center of Montgomery County (Virtual)
November 16: 1:00 PM to 3:00 PM

Complete calendar of events **online**

Virtual Forum 2021 – Alzheimer's Disease & Related Disorders

Over 400,000 individuals are living with Alzheimer's Disease or a related disorder in the commonwealth and the toll of this disease extends beyond those affected to their families, friends, and communities.

The Department of Aging is hosting the 2021 Alzheimer's Disease and Related Disorders Virtual Forum: Physician and Consumer Education in Early Detection, Diagnosis, and Treatment on **November 4 from 9:00 AM – 12:30 PM**.

Tina Kotsalos, Director, Investor Education and Consumer Outreach for DoBS, will participate on a Financial Exploitation Education Panel.

Learn more and register.

Beware of Student Loan Forgiveness Scams

The Pennsylvania Department of Banking and Securities (DoBS) and Pennsylvania Department of Education (PDE) are warning consumers to be wary student loan forgiveness scams.

The COVID-19 pandemic has caused financial struggles for many borrowers who are seeking relief. If a student or borrower receives an email, letter, or call about student loan debt forgiveness, they should pause before sending or confirming any personal information.

Take the following actions to help safeguard against these types of scams:

- **Be skeptical**. Scammers often obtain student loan information illegally. Just because someone has information about your loans, doesn't mean they are to be trusted.
- **Research the company**. Check the validity of the company contacting you as many "companies" run by scammers do not actually exist.
- **Do your due diligence**. Check what program is being offered to you. Some scams offer to enroll you in programs like the "CARES Act loan forgiveness" or the "Biden forgiveness program," neither of which exist.
- **Verify that email address**. Ensure that emails being sent to you about your student loans are from a dot-gov (.gov) email address.
- **Be aware of what legitimate programs will and won't ask you for**. Proceed with caution before sharing any of your sensitive or financial information like a Social Security Number or credit and bank information. If in doubt, hang up and call your servicer directly.
- **Pause before taking action**. Confirm any correspondence or calls with your servicer before taking any action.

Think you've been scammed?

- **Close Accounts/Stop Payment**. If you shared your bank account or credit card information with a scammer, contact your bank or credit card company immediately to close your accounts or stop payments.
- **Alert your servicer**. If you suspect you've been the victim of a student loan forgiveness scam, call your servicer so that they can monitor your account.
- **Monitor your credit report**. Check for suspicious activity. Scammers don't always use your information right away. It can be weeks, months, or even years before your information is used for fraudulent activity. You might also consider freezing your credit in an abundance of caution.
- **Report the scam**. You can report a student loan forgiveness scam to:
  - » Federal Trade Commission
  - » Pennsylvania Attorney General

DoBS outreach professionals Katrina Boyer (left) and Tina Kotsalos (right) are joined by Attorney General Josh Shapiro at the Abington Pre-Night Out Event at the Abington Town Center in Montgomery County on August 2.

Contact DoBS...

Call **1.800.PA.BANKS** or 800.600.0007 or online to ask questions file complaints about financial transactions, companies, or products.

Schedule outreach events by contacting us at informed@pa.gov.

If you believe you have fallen victim to a scam, contact local law enforcement.

In August, the department partnered with the Penn State Extension to launch a free, online program to help farmers with retirement planning. Farmers had the opportunity to learn about investment strategies, fraud awareness, planning, budgeting and saving for the future during the multi-session program. Penn State Extension is a modern educational organization dedicated to delivering science-based information to people, businesses, and communities. They make a difference locally through focused engagement, and more widely to customers connecting in the digital landscape.

Recordings of the programs can be viewed:

- Farmers Can Retire Too: Budgeting, Planning, and Saving
- Farmers Can Retire Too: Retirement Planning

Interested in offering your group one of our programs? The DoBS Investor Education and Consumer Outreach staff is here to help! They can work with your group to offer one of our free programs or presentations or can tailor a program to your specific needs.

Contact informed@pa.gov to learn more.

Compliance Corner

3rd Quarter 2021 Enforcement Orders

The department protects consumers through the following laws:

- **Check Casher Licensing Act**
- **Consumer Credit Code**
- **Consumer Discount Company Act**
- **Credit Services Act**
- **Debt Management Services Act**
- **Debt Settlement Services Act**
- **Loan Interest and Protection Law**
- **Money Transmitter Act**
- **Mortgage Licensing Act**
- **Pawnbrokers Licensing Act**
- **Pennsylvania Securities Act of 1972**

The Department of Banking and Securities issued **42 enforcement orders** during the third quarter of 2021 from July to September 2021. **Fines and assessments for these orders totaled $894,550**. To see details on these enforcements, visit the Enforcement Orders section of the department's website.

Join the Conversation...

If you haven't checked out the Department of Banking and Securities on social media lately, you're missing out!

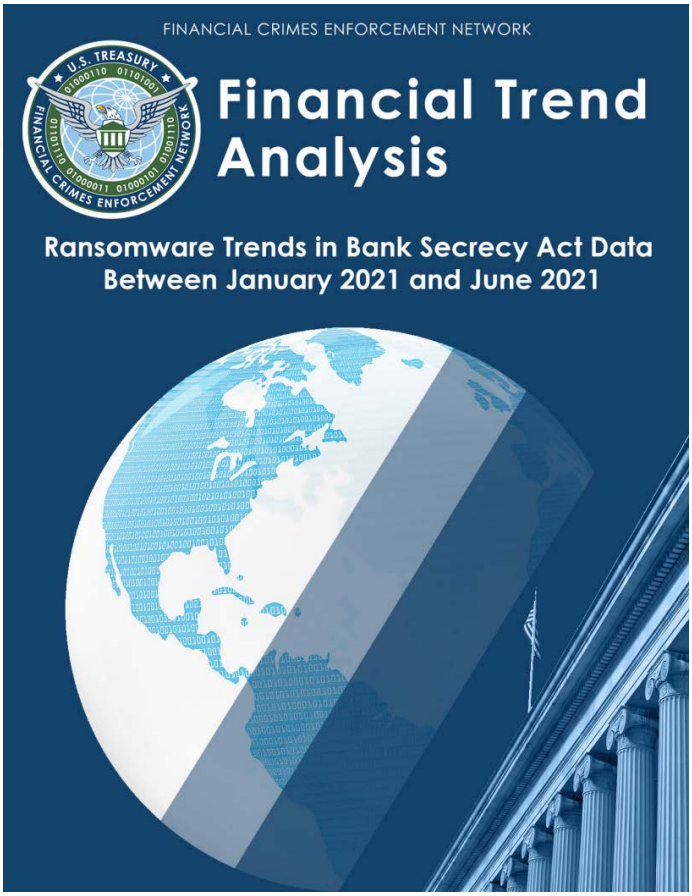
Follow us at our Twitter handle for news and conversations relevant to the PA financial industry: @PADeptBanking

Like our new, active Facebook page for videos and infographics about protecting and managing your money: PA Banking and Securities

Connect on LinkedIn for employee news, job openings and tips for finance professionals: PA Banking and Securities

The Cyber Section

FinCEN Releases Ransomware Trends Analysis



The U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) released a report earlier this month analyzing ransomware trends during the first six months of 2021.

According to the new report, more than 450 ransomware payments were reported to FinCEN from January to June 2021, with more than $590 million having been paid to attackers. This was a large increase over the previous year which saw $416 million paid all of 2020.

The report includes guidance by FinCEN on detection, mitigation, and reporting of ransomware incidents.

"Financial institutions play an important role in protecting the U.S. financial system from ransomware related threats through compliance with BSA obligations. Financial institutions should determine if a SAR filing is required or appropriate when dealing with a ransomware incident, including ransomware related payments made by financial institutions that are victims of ransomware.43 Financial institutions may also file with FinCEN a report of any suspicious transaction it believes relates to the possible violation of any law or regulation but whose reporting is not required by 31 CFR Chapter X."

Read more: FinCEN Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021

Updated Online Cybersecurity Guide

The commonwealth's online cybersecurity guide, Protecting Yourself Online, was recently updated to include new information about cybersecurity while teleworking and online safety for children and teens. The guide and its updates are a collaboration of the Department of Banking and Securities, Insurance Department, Department of Revenue, Office of Administration, and Office of Attorney General.

In addition to the most recent updates, the guide includes helpful resources and guidance on reviewing your credit report, filing a complaint, reporting identity theft, creating safe passwords, and more.

Visit the Protecting Yourself Online guide.

New Federal Ransomware Website Launched

Federal agencies have partnered to launch a new website providing resources to help organizations defend themselves against ransomware.

StopRansomware.gov offers information on the threat of ransomware, mitigate risk, and what to do in the event of an attack. The website includes reports, alerts, and other resources from CISA, the FBI, and other federal partners that can help with ransomware protection, detection, and response.

Visit StopRansomware.gov for more information.