Testimony of Charles G. Cooper Commissioner
Texas Department of Banking
House Committee Business and Industry
June 9, 2016

Good morning Chairman Oliveira and distinguished members of the committee. I would like to make a few brief remarks and then introduce you to Phillip Hinkle, our Department's Director of IT Security Examinations.

The Committee is charged with identifying and addressing potential gaps in Texas businesses' cybersecurity policies and ensuring that Texans' personal information held by these businesses is secure. I would like to share how the Department of Banking has been working on cybersecurity with our financial institutions to ensure that not only the banks are protected, but the citizens of Texas as well.

Cybercrime continues to grow at an alarming pace and affects all of us. It is certainly an issue for the banking industry but also for all businesses and individuals as well as our infrastructure.

Banks are at the forefront of financial crimes, as they are the guardian of funds and are typically the first point of attack. Bad actors [criminals] have always been around. Willie Sutton, a famous bank robber with a 40 year career, was asked at the time of his arrest why he chose banks to rob. His answer was simple, "That's where the money is."

In some cases, cyber criminals target account holders in an effort to compromise the customer's account and gain access to their funds. In other instances, the financial institution is the direct target. It is important to understand that if a consumer's funds are stolen, regardless of who the criminals target, the consumer is protected under Regulation E. Businesses, however, have a duty to protect their computer systems and are not covered under Regulation E. If they are targeted and have not protected their computer system, courts have rules in several cases that the business is at fault. Naturally, if the bank is targeted and compromised, they would shoulder the financial lost. Increased security awareness for business owners when conducting business transactions is important, not only with banks, but with everyone.

We at the Department of Banking have been diligently working with the industry to increase awareness and ensure that financial institutions have the proper defense in place to manage not only their computer systems, but to also help protect businesses that are not protecting themselves. We recognize that this is an increasingly difficult battle. The Department created the Texas Bankers Electronic Crime Task Force in 2010 with the U. S. Secret Service. We originated several programs in Texas, which have expanded nationally through the

Conference of State Bank Supervisors, an organization where I currently serve as chairman.

For further insight into how the Department conducts its campaign on cybersecurity and awareness projects, I would like to introduce an expert in the area of cybersecurity. Phillip Hinkle is the Director of IT Security Examinations for the Texas Department of Banking. He has a variety of IT certifications and has been with the Department for 27 years.

He received the FBI's Service Award for his work in this field. He currently serves on the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity and Critical Infrastructure Working Group (CCIWG). FFIEC is composed of federal banking regulatory agencies. Phillip Hinkle represents the states in the CCIWG and is one of the six voting members.

# House Committee on Business and Industry

June 9, 2016

# Cybersecurity

Phillip Hinkle, Director of IT Security Examinations

Texas Department of Banking

# U.S. Government Position on Tackling Cyber Threats

- **Cyber threats are too large** for any one government agency or company to address.
  - private and public partnerships are needed.
- **We hear this same message from:**
  - James Comey, the current FBI Director
  - Robert Muller, the former FBI Director
  - Michael S. Rogers, the current NSA Director
  - Keith Alexander, the former NSA Director
  - Jeh Johnson, the current DHS Secretary
  - Janet Napolitano, the former DHS Secretary
  - John Brennan, the current Director of the CIA

# Partnership on Cybersecurity

- Information Sharing and Analysis Centers (ISAC) are industry specific forums for sharing threat information and solutions related to cyber threats.
- FS-ISAC is the largest and most advanced ISAC in the world. It is a partnership of the financial services industry. A non-profit, industry owned organization.

# Partnerships of Texas Banks

- In 2010, Commissioner Cooper created the Texas Bankers Electronic Crimes Task Force (ECTF).
- The ECTF includes members of bank trade associations, approximately two dozen banks, and the U.S. Secret Service.
- Working with ECTF Texas banks, the U.S. Secret Service launched “Operation Texas Money Mule,” a global undercover operation.

# Partnerships of Texas Banks

- The task force developed Corporate Account Takeover (CATO) Best Practices, which were nationally distributed by the U.S. Secret Service, FS-ISAC, and the Conference of State Bank Supervisors (CSBS).
- CATO Best Practices have been adopted by banks nationally to help protect small businesses, consumers, and banks.

# Executive Leadership of Cybersecurity (ELOC)

- In late 2013, Commissioner Cooper reconvened the Texas Bankers ECTF with numerous presidents and executive officers of banks and trade associations.
- The reconvened task force provided input for what became the Executive Leadership of Cybersecurity (ELOC) initiative.

# Executive Leadership of Cybersecurity

- Working with the CSBS, the ELOC initiative was launched nationally in December 2014 in Austin, Texas.
- The U.S. Treasury Department supports the initiative and Deputy Treasury Secretary Sarah Bloom Raskin was the keynote speaker.
- FS-ISAC President Bill Nelson spoke at the national launch.
- FS-ISAC supports the initiative .

# Executive Leadership of Cybersecurity

- In 2015, ELOC events were held in approximately 20 states and presented to over 2,000 bankers.  Events continue to be scheduled in 2016 in other states.
- ELOC is the single most important transformational element to secure the banking industry from cyber threats.

# Federal Cyber Regulations & Activities

- Since 2006, states have had a voting position on the Federal Financial Institution Examination Council (FFIEC).
- In 2013, the FFIEC established the Cybersecurity and Critical Infrastructure Working Group (CCIWG) as a permanent structure.
- The Texas Department of Banking's Director of IT Security Examinations is one of the six voting members of the CCIWG.

# Federal Cyber Regulations & Guidance

- Before cybersecurity, there was information security.
- Information security has been a part of bank examinations since the 1970s.
- In 1999, the Gramm-Leach Bliley Act (GLBA) established comprehensive bank regulatory standards for information security.

# Gramm-Leach-Bliley Act 15 USC 6801

**TITLE 15 , CHAPTER 94 , SUBCHAPTER I , Sec. 6801.**

**Sec. 6801.** - Protection of nonpublic personal information

(a) Privacy obligation policy

… each financial institution has an affirmative and continuing obligation to …protect the security and confidentiality of … customers' nonpublic personal information.

(b) Financial institutions safeguards

… each agency … shall establish appropriate standards for the financial institutions …relating to administrative, technical, and physical safeguards -

(1) to insure the security and confidentiality of customer … information;

(2) to protect against any anticipated threats …to the security …of such records; and

(3) to protect against unauthorized access …of such records …

**Numerous regulations and guidance letters have been issued over the years.**

# Federal Cyber Regulations & Activities

- The FFIEC has held cybersecurity webinars attended by thousands of bankers.
- In June 2015, the FFIEC released a Cybersecurity Assessment Tool (CAT) to assist banks in measuring their cyber risks and preparedness.

# Department Actions

- Texas state-chartered banks were directed to complete a cybersecurity risk assessment and evaluation of controls by the end of 2015.
- In 2016, the Department began evaluating Texas state-chartered banks readiness in meeting the new FFIEC “baseline” cybersecurity level.
- Early results of the Department’s review for FFIEC baseline controls show that Texas’ state-chartered banks are addressing cybersecurity risk.

# Conference of State Bank Supervisors

(http://www.csbs.org/CyberSecurity/Pages/default.aspx)