Is Your Bank Ready for a Visit from Jesse James and the Gang?

By W. Scott Evans and James W. Lane Jr., Flaherty Sensabaugh Bonasso PLLC

West Virginia folklore has it that Jesse James and his band of outlaws robbed the Bank of Huntington on September 6, 1875. According to the Huntington Advertiser, the amount taken from the bank was between $19,000 and $20,000.

While recent attention has focused on cyber-crimes that threaten banks and banking infrastructure, it is just as important to be prepared for old-fashioned crimes like those committed by Jesse James and his gang of outlaws. Significantly, the last five years of the FBI's bank crime statistics indicate that bank robberies have occurred on average 4,132 times per year nationally, which roughly translates into one bank robbery every two hours. From a local standpoint, it is important to note that bank robberies occur on average more often in the Southern United States. While businesses face an ever-increasing risk of cyber-crimes, bank robberies still pose a real threat that banks must be prepared to address. This article will examine some of the key legal and regulatory issues banks encounter due to the threat of crime and crime-related injuries to bank personnel and customers, as well as preventative measures banks should consider to reduce exposure.

Under West Virginia law, it is possible for an employer such as a bank or credit union, to be held liable to an employee who suffers damages because of the criminal conduct by a third-party. In addition to the risk of legal liability for injured employees, an injured third-party, such as a bank customer, may bring civil action for injuries that result from a robbery. There are reported court decisions involving plaintiffs who have brought negligence claims based on the standards and requirements set by Congress in the Federal Bank Security Act of 1968 ("BSA"). This Act requires, in part, that banks adopt "appropriate security procedures to discourage robberies/burglaries" and holds a bank's Board of Directors responsible to ensure the development and implementation of a "written security program for the bank's main office and branches." Litigants have used evidence of a bank's failure to meet their minimum-security standards to establish liability for a bank customer's injury. Therefore, considering this exposure, banks should update their security threat preparation and training, using the general security requirements of the BSA and its accompanying regulations as a minimum threshold.

Furthermore, FDIC regulations direct that the bank's Board of Directors must designate a security officer "who shall have the authority, subject to approval of the bank directors to develop and to administer a written security program for each banking office." FDIC regulations outline the general contents of a security program which are to include:

1. Procedures for opening and closing;

2. Procedures to assist in identifying persons committing crimes, such as cameras, and the use of identification devices such as pre-recorded serial-numbered bills, or chemical and electronic devices;

3. Provide for initial and periodic training of officers and employees; and

4. Provide for selecting, testing, and operating and maintaining appropriate security devices.

FDIC regulations further identify the minimum requirement for security devices which should include, in part:

1. A vault, safe or other secure space;

2. A lighting system to illuminate the area around the vault if the vault is visible from the outside of the bank;

3. An alarm system for prompt notification of law enforcement;

4. Tamper resistant locks on the exterior doors and windows; and

5. Other such devices as the security officer determines appropriate based upon the amount of currency or valuables on site, the distance of the bank from law enforcement, the cost of security measures, other measures utilized in other banking offices, as well as the physical characteristics of the bank itself.

Finally, regulations for the Bank Protection Act require that the security officer must report at least annually to the bank's Board of Directors on the "implementation, administration, and effectiveness of the security program." Thus, the Bank Protection Act of 1968 and its accompanying FDIC regulations provide critical guidance as to the general matters to be covered by a security plan, but it is important that it only provides a floor for the security measures that must be implemented.

Considering this legal landscape, banks should implement the most up-to-date measures and technology as part of an overall global security strategy to assure that their employees and banking customers have a safe banking workplace and environment:

1. **REGULARLY UPDATE WRITTEN SECURITY PROCEDURE –** As required by the Bank Protection Act, banks must have a security plan with written policies and procedures designed to provide a safe work environment for staff and a secure banking facility for customers. Procedures should outline in detail the security-related training to be conducted with each new and current employee, outline the bank's security equipment reviews and maintenance, and require routine internal and external security auditing. All security training and assessments should be thoroughly documented by the bank's security officer.

2. **CRIMINAL ACTIVITY ASSESSMENTS –** Banks and their security team members must continually update and document their assessment of local criminal activity in their bank locations. The security team should examine if there has been an increase of bank-related crime, including criminal activity targeting customers in bank parking lots or while using bank ATM's. An increase in crime for a particular location may require the bank to identify and implement additional protective measures.

3. **ENGAGE LAW ENFORCEMENT –** A bank's security officer should engage in ongoing consultation with law enforcement regarding local criminal activity. Bank security should request that the local FBI or other law enforcement agencies conduct regular staff training sessions to ensure bank employees remain current with the most up-to-date measures to reduce the risk.

4. **SELF-AUDITS –** Security audits and reports should be conducted routinely to determine whether the most current risk protection technology and practices are being incorporated. Security programs should always reflect an evolving strategy that adapts to ever-changing criminal threats.

5. **DOCUMENT ALL SECURITY TRAINING –** Should litigation result, a key piece of a bank's defense will be documentation related to the security program, planning and training, all of which must satisfy at a minimum, the requirements of the Bank Protection Act as well as demonstrate that the bank's security program has incorporated the most appropriate risk management practices.

The above suggestions are starting point for banks to consider when addressing security issues. Criminals, like Jesse James and his gang, will always consider banks as a prime target. Therefore, it is important that banks appreciate the public's high expectation of bank security and need not only aim at satisfying the minimum standard set by federal law but strive to exceed those requirements to protect their staff and patrons. If a bank fails in implementing a robust and proactive security program, their Board of Directors run the real risk of twelve jurors judging whether security measures were up-to-date, appropriately planned and properly implemented – a risk that ultimately may not be favorable to the bank's reputation or bottom-line. ■

Scott Evans is an attorney with Flaherty Sensabaugh Bonasso. He is a veteran defense attorney with over 20 years of litigation experience. Scott focuses his practice in the areas of employment law and corporate defense. He can be reached at 304.347.4214 or wsevans@flahertylegal.com.

Jim Lane is an attorney with Flaherty Sensabaugh Bonasso. With more than 20 years of experience in financial services law, Jim's focus is bankruptcy, creditors' rights matters, business transactions and business-related disputes. He can be reached at 304.205.6373 or jlane@flahertylegal.com.