Texas Bankers Association
Strong Banks. Stronger Communities.

ATM CRIME TASK FORCE **REPORT**

NOVEMBER 2020

ATM CRIME TASK FORCE BACKGROUND & **MISSION**

In the late summer and fall of 2020, TBA began to receive an increasing number of communications from member banks reporting Automated Teller Machine (ATM) “smash and grab” crimes. These aggressive attacks are dubbed “smash and grab” as incidents share several common signatures and violent traits. Perpetrators typically use stolen construction vehicles or heavy-duty trucks and chains to rip apart ATM encasements to access cash canisters. Vehicles may also be used to tear machines from their platforms altogether to steal the machines and haul them away largely intact. In particularly egregious cases, criminals used trucks to crash into closed grocery or retail stores to access bank ATMs located inside.

Houston and Southeast Texas have been recognized for several years as hotbeds for ATM crime, with a special law enforcement unit composed of FBI and local law enforcement personnel focusing on the crime in the region. But it became clear during the 2020 pandemic that the threat had increased dramatically and that banks in other parts of Texas had become targets. Further, banks observed that criminals had become more sophisticated in their methods as evidenced by the rapid speed at which the attacks were being carried out (sometimes just 2 – 3 minutes).

In October, additional indicators of the seriousness of this issue appeared. On October 16, 2020, the FBI issued a Private Sector Liaison Information Report indicating that ATM criminals across the US had taken the attacks to another level by utilizing explosives to breach ATMs. The use of this tactic was disturbing as it raised concerns not just for the loss of cash and total loss of the machine, it more importantly represented a larger potential threat to the safety of bank employees and customers. Two of the examples cited in the FBI report were from Texas.

Also, in October, an insurance carrier providing coverage for Texas banks alerted TBA’s Bankers Insurance Agency that they were experiencing losses at such a rate that it could soon impact bank policy deductibles and premiums.

It was clear that action was necessary.

TBA alerted member banks of the growing threat and began to actively solicit banks to report ATM crime incidents and to provide as much detail as possible. Within just a few days, the TBA

member relations team had collected more than 100 incident reports from banks across a wide geographic footprint in Texas.

After outreach to law enforcement officials and other vital stakeholders, TBA announced the formation of the ATM Crime Task Force at the virtual Security and Risk Management Conference on November 5.

The ATM Crime Task Force includes Texas bank executives and security leaders representing OCC-regulated institutions, state-chartered banks, and thrifts. TBA was grateful for the active engagement of Commissioner Charles Cooper of the Texas Department of Banking and Commissioner Caroline Jones of the Texas Department of Savings and Mortgage Lending as well as representatives of law enforcement agencies, the insurance industry and an ATM manufacturer.

The objectives of the ATM Crime Task Force:

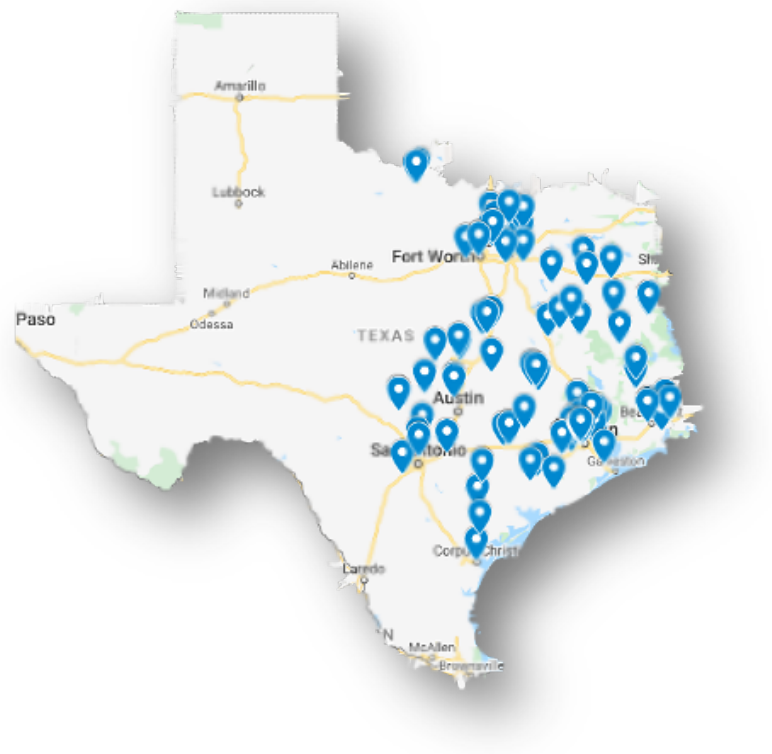
- Increase awareness and information sharing about the extent and nature of these crimes across all stakeholder groups
- Strengthen relationships between banks, key stakeholders, and law enforcement
- Discuss deterrents and mitigating solutions for both the near and long-term
- Explore possible machine protective measures and design changes
- Understand the insurance impact for Texas banks

On Monday, November 16, 2020, the ATM Crime Task Force met via Zoom. This summary captures key findings and recommendations provided by the outstanding group of stakeholders taking part on the Task Force.

KEY TASK FORCE **FINDINGS**

KEY FINDING: ATM CRIME IS SPREADING RAPIDLY IN TEXAS

At the ATM Crime Task Force meeting, TBA presented a heat map of ATM crimes reported to the association. It revealed at least 139 incidents over the last 12 months. It is clear that this is a sample and does not constitute the full breadth of incidents. While concentrations in southeast and east Texas were somewhat expected, it was evident that these attacks have migrated on a large scale into Central Texas as well as the Metroplex, north and northeast Texas. Few reports have come from the Valley, West Texas and the Panhandle to date, but this situation cannot be expected to continue. Since the Task Force meeting, banks have continued to report additional hits pushing the total number of reported ATM crimes over the 150 mark. If your bank has not sustained a smash and grab attack, it may only be a matter of time. The heat map illustrated that ATM crime is no longer a just problem in the Houston metro area. It is a Texas problem and a growing national issue.



Map of Texas ATM Crimes

KEY FINDING: ORGANIZED CRIME IS AT THE ROOT OF SMASH AND GRABS

Organized crime is the predominant source of ATM criminal activity in Texas, and approximately 95% of these groups are based in the Houston area. However, as previously stated, they have expanded their activities not only within Texas but into neighboring states. In mid-November, local law enforcement officials in Edmond, Oklahoma apprehended an ATM "Smash and Grab" criminal suspected to have ties to a Houston-based organization. Reports indicate that Brandon Gonzalez, 27, had attempted to burglarize an ATM using a stolen truck and chains. He was charged with breaking into the ATM, Felony Pursuit, Obstruction, and Possession of a Stolen Vehicle. Houston-based FBI officials taking part in the Task Force meeting say that they have made more than 50 arrests and are actively tracking about 250 individuals suspected of being part of these criminal rings.

KEY FINDING: ATM CRIME LIMITS COMMUNITY ACCESS TO FINANCIAL RESOURCES DURING THE PANDEMIC

The hits on TBA's ATM crime heatmap have taken place within the last year, with most occurring during the COVID-19 emergency. Many bank lobbies have been closed or restricted during the pandemic and banks and their customers depend more on ATMs and Interactive Teller Machines (ITMs) to conduct transactions. When these machines are damaged or destroyed, it may take weeks before they can be repaired or replaced. Smaller communities and those with a limited number of financial institutions and fewer law enforcement resources are particularly impacted. The bottom line is that ATM crime limits the access that citizens have to their financial resources during the pandemic. This is not just a crime against banks, it is a crime against the community.

KEY FINDING: ATM CRIME IS DRIVING MILLIONS IN LOSSES FOR TEXAS BANKS AND THEIR INSURANCE CARRIERS

Law enforcement partners estimate that Texas banks have experienced close to $13 million in cash losses due to ATM theft. Banks participating on the Task Force report that just one or two of these crimes can lead to losses into the multiple six figures for an individual bank. Even unsuccessful attempts to breach an ATM cash cartridge can cause significant losses for banks and their insurance carriers due to the destruction of equipment. ATM costs vary, but the average machine purchase price is $35,000 – 40,000. Many community banks seeking to enhance the remote customer experience through the use of ITMs may spend on average $75,000 – 80,000 or more on a machine. ITMs can also hold more cash. When the cost of equipment damage is combined with cash losses, the total estimated ATM smash and grab losses in Texas skyrocket to $24 million.

Insurance companies have expressed their concern about the rising costs and the impact it may have on their bank customers. If current trends continue to worsen, significantly higher insurance deductibles and premiums may result. Further, should criminals expand the use of explosive devices to breach ATMs and ITMs, there is the potential for employee or customer loss of life that no insurance policy can replace. Taking steps to reduce the severity and frequency of these attacks will be critical to keeping insurance costs, and all costs related to Smash and Grab crimes, in check.

RECOMMENDATIONS FOR **TEXAS BANKS**

In order to reduce the frequency and severity of ATM crimes, the ATM Crime Task Force considered criminal tactics and recommended a number of actions and leading practices to

address specific risk factors or to enhance collaboration to combat them. These recommendations include:

FOCUS ON YOUR RELATIONSHIP WITH LOCAL LAW ENFORCEMENT

Having a relationship with local law enforcement agencies is critical to fighting ATM crime. Law enforcement should not be viewed simply as providing a response capability, they should be considered a vital partner in helping to deter and prevent ATM attacks and other bank crimes.

A strong relationship will include established points of contact, confirmation of all bank ATM locations and infrastructure as well as regular communication about concerns that law enforcement or the bank may have. If you already have a strong relationship with law enforcement in your area, you will see in the following recommendations that there are other ways that banks and law enforcement may collaborate to specifically reduce ATM crime risk.

ENSURE THE BASICS AND ASSESS YOUR RISK

Properly securing ATM machines—with bolts into concrete, for example—and ensuring that areas surrounding ATMs are well-lit are basic measures. However, as these crimes proliferate and smash and grabbers get more sophisticated, more must be done.

An important step in effectively protecting these valuable pieces of equipment and the cash they hold is to assess vulnerabilities. If your bank does not have professional security personnel on staff or a formal relationship with a security consulting firm, the American Bankers Association's *ATM Security Risk Assessment Tool* may be helpful to you. The tool highlights key security considerations and enables banks to rate their level of risk. You can find this tool in the resources section of this report.

POSITION BOLLARDS AND BARRIERS—PARTICULARLY ON OUTSIDE LANES AND ISLANDS

Criminals need space to position vehicles or gain leverage for the quick execution of their crimes. ATMs that are stand-alone, that are located on outside bank lanes or on traffic islands are far more vulnerable to smash and grab attacks. Strategically positioning bollards or barriers around ATMs can serve as a visual deterrent and can make their efforts more difficult and time consuming. If your risk is great, you may also consider relocating ATMs altogether to more secure locations or consider positioning ATMs as wall units.

CONSIDER MACHINE ENHANCEMENTS: HEAVY-DUTY BARRIERS, GATE & DOOR KITS, GPS TRACKERS

Talk to your ATM provider about the addition of security enhancements to your existing machines. Criminals are counting on being able to breach the machine in three minutes or less. Bolstering the immediate machine perimeter with heavy-duty barriers, utilizing gate and door kits or deploying other visual

reinforcements can significantly delay their ability to be successful. One manufacturer, for example, has re-designed ATM safes specifically for island units. You may also consider the addition of GPS trackers in case criminals are able to extract cash cassettes.

EVALUATE YOUR ALARM SETTINGS AND SENSORS

If law enforcement response may be delayed by distance (in rural areas, for example), piercing audible alarms may be preferable to silent alarms to startle the perpetrators and encourage their rapid departure. Conversely, in cities or areas where the law enforcement presence may be greater and response may be faster, silent alarms may be best to allow police the opportunity to catch the criminals in the act. Understanding the dispatch process and typical response times in your local community should be a part of your discussions with law enforcement about your ATM locations. This will help you choose the settings most appropriate for each machine. If possible, consider testing alarms and response times in coordination with law enforcement. Adding security enhancements, such as gates, vibration and heat sensors, may support faster alarming capabilities.

BE UNPREDICTABLE

Law enforcement officials and bank security experts say ATM criminals are surveilling bank targets before they strike. A bank may be cased just a few hours before a smash and grab attempt. But the criminal organizations behind smash and grabs may utilize local accomplices to provide information about bank employee habits as well as to develop “intel” on law enforcement patterns, shift changes, and response times. Be unpredictable. For example, work with employees and vendors to service machines and replenish cash cassettes on alternating schedules. Train staff to be mindful of activity around them at all times and to report suspicious activity or individuals to local law enforcement.

MAKE THE MOST OF CAMERAS

Do you have only a few cameras with limited lines of sight? Criminals surveilling banks will evaluate the number of visible cameras and their positioning. Ensuring that your bank’s camera system is able to capture a number of angles and include adjacent properties, parking lots, roads, etc. will increase odds that law enforcement can use camera images/ video to not only capture the crime, but to spot and identify criminals and “switch” vehicles that may be standing-by in close proximity. While there is expense to these and other security enhancements, one ATM attack can cost much more.

PROPERLY “CODE” ATM CRIMES

Should your bank be the victim of an ATM smash and grab attack, be sure that law enforcement properly documents and codes the crime. For example, smash and grabs are violent theft attempts often using stolen vehicles and costing banks tens of thousands of dollars. They are not simply acts of vandalism or property damage. This is another topic of

discussion to have with law enforcement before you are the victim of such a crime. Ensure that law enforcement is aware of Sec. 31.03 of the Penal Code, Texas' theft statute. It was amended in recent years to specifically include the theft of automated teller machines or their contents. As mentioned later in this report, TBA is pursuing additional enhancements to state and federal law.

CONSULT YOUR INSURANCE PROVIDER

Discuss your policy and clearly understand what it covers—and as important—what it will not cover. Ask about the Financial Institution Bond that covers cash located in the machine and about the separate Commercial Package policy that covers physical ATM damages. Communicate to your provider the proactive defensive measures your bank is taking to reduce the risk.

BANKER-TO-BANKER INFORMATION **SHARING**

Without information shared by TBA bank members, the extent and scale of ATM smash and grab crime in Texas would still be flying below radar, even as the risk and costs increased. Please continue to report ATM crimes to TBA as it enables us to work more effectively with law enforcement, elected officials and your fellow bankers to fight this costly scourge.

Please consider joining TBA's TruStar information sharing network. Using this secure Texas bank-to-Texas bank intelligence platform comes at NO COST to TBA member banks. It is also being used to counter skimming/card fraud crime and cyber threats. Contact Alvin Mills, TBA VP for IT & Security, to learn more: alvin@texasbankers.com

POSSIBLE LEGISLATIVE **ACTION**

The theft or attempted theft of an ATM are federal and state crimes. However, there is room to increase criminal penalties as enhanced deterrents and as additional prosecutorial tools for charging and convicting ATM criminals.

In urban areas where ATM smash and grab crimes have become commonplace, law enforcement often pursues federal bank robbery charges against perpetrators. ATM thefts and the crimes committed incidental to the robbery are federal crimes under 18 U.S.C. §2113. The challenge, however, is that once police and law enforcement agents have done their jobs, prosecution of these crimes may be seen as low priorities by some prosecutors. TBA will work

with the Texas Congressional delegation to determine how federal penalties can be enhanced to adequately deter these crimes. Further, we will reach out to US attorneys to encourage prosecution by raising awareness of the growing breadth, economic cost, and community impact of ATM crime.

Meanwhile, the Texas Legislature is set to meet beginning January 12, 2021, and TBA has already begun to work with legislators to amend Sec. 28.03, the Texas criminal mischief statute, to clearly provide that the damage to or destruction of an automated teller machine is a third degree felony, which is punishable by 2-10 years in prison and a fine of up to $10,000, or both.

RESOURCES FOR **TEXAS BANKS**

The FBI's Violent Crimes Task Force in Houston has provided a **briefing** on ATM crimes to include field observations and ATM crime data. Access it **HERE**.

As mentioned in earlier in this report, the American Bankers Association has developed an **ATM Risk Assessment Tool**. Bank security executives can find it **HERE**.

Countering Smash and Grab ATM attacks were the cover feature in the November 2020 issue of TBA's *Texas Banking* magazine. Read security expert Barry Thompson's outstanding article with **additional security recommendations HERE**.

In this **TBA VIDEO**, Brien O'Connor, a former law enforcement officer and President of TBA's Bankers Insurance Agency provides ATM **insurance tips**. You may reach Brien at: brien@bia.insurance.

CONCLUSION

The crisis that was the Great Depression of the 1930's saw an increase in bank robberies that resulted in TBA's establishment of a reward program for the apprehension of criminals. While the criminal justice system and reward requirements have certainly changed, the historic reward program continues to this day, aiding law enforcement in the capture and prosecution of bank robbers across Texas.

The COVID-19 pandemic has likewise seen the rise of modern-day theft in the form of ATM crime. TBA is acting to meet this contemporary challenge for our Texas banks and your input, participation, and ideas are strongly encouraged.

The ATM Crime Task Force meeting was but a first step. TBA will continue to work with Task Force members, law enforcement, regulators, legislators, and, most importantly, our bank members to track these crimes, to develop countermeasures and deterrents, and to reduce the frequency and severity of the attacks.

ACKNOWLEDGEMENTS

The Texas Bankers Association gratefully acknowledges the participation and contributions of the following individuals in support of the ATM Crime Task Force. We thank them for their leadership and collaboration to unite our efforts and develop effective solutions to counter these crimes in Texas.

Texas Department of Banking:
Commissioner Charles Cooper

Texas Department of Savings and Mortgage Lending:
Commissioner Caroline Jones

Federal Bureau of Investigation:
Kelly Olson
Christal Swagerty
Torrence White

Houston Police Department:
Jose Garcia
Kerry Richards

Extraco Banks: Christopher Kincaid

Commercial Bank of Texas: Raymond Rust, III

First National Bank Texas: Bobby Maxwell

Industry State Bank: Lisa Moeller

International Bank of Commerce: Kevin Mullins

JPMorgan Chase Bank:
David Emerick
Kevin Preola
Steve Flowers

Providence Bank of Texas: Randy McCauley

Rio Bank: Rodney McElrath

Shelby Savings Bank: William Lucas

Southside Bank: Russell Estrada

Texas Bank and Trust Company: Pam Mitchell

TFNB Your Bank for Life: DJ Adams

The First State Bank:
William Jenkins, III
John “JC” Bouse

Bankers Insurance Agency: Brien O'Connor

OneBeacon: Craig Collins

NuSource Financial: Jon Erpelding

Texas Bankers Association:
Chris Furlow
Celeste Embrey
Michele Carfello
Brent Cox
Mary Lange
Zach Malone
Alvin Mills