

# **SAFECATCH**

**STOP THIS ROBBERY**

**STOP THIS ROBBERS FUTURE ROBBERIES**

**TRAINERS MANUAL**

## **BACKGROUND**

### ***Bank robbery in the Puget Sound.***

By the mid-nineties, the Seattle Division of the FBI was recording more than 300 bank robberies a year. This consistently placed the state of Washington as one the most robbed states in the country. In response to this rising rate of bank robbery, the Division created the Puget Sound Violent Crimes Task Force. Coinciding with the task force the Washington Bankers Association successfully lobbied the Washington State Legislator for increased penalties for note passers. Note passers accounted for well over 90% of the bank robberies in the state. These efforts have been some what successful; however, they have not relieved bank employees from the burden of working in an environment where robbery is still far too common. For example, in 2006, Washington State recorded 287 bank robberies. This ranked the Seattle area fourth in the United Sates for most bank robberies.

In response to this decades old problem, the Seattle Division began forwarding the idea that bank employees could safely do far more in preventing and partnering with law enforcement than traditionally believed. To accomplish this, the Division's Bank Robbery Coordinator teamed up with Security Managers from various Seattle financial institutions and developed what is today referred to in the banking industry as SAFECATCH.

## **SAFECATCH**

### ***Special note with regard to the safety of bank employees***

SAFECATCH, an acronym, is a two pronged bank robbery suppression program. The SAFE prong is a preventive measure; the "CATCH" prong is designed to partner bank employees with law enforcement. Together, they bring a comprehensive plan to the industry which creates an environment that empowers bank employees to make a difference.

When developing this program, bank robberies were carefully researched from 1996 thru 2006. Of specific interest where bank robberies where acts of violence occurred, from assaults to death. This research was of

great importance to ensure that utilizing customer service skill's as robbery prevention tools was safe for employees. The research did not reveal any situations or circumstances where a robber entered the bank posing as a customer, was treated as customer and the robber then subjected that employee to violence.

There is no confrontation aspect within the SAFECATCH program. The strategies trained do one of two things, provide great customer service that opens the door to build a business relationship; or provides a potential bank robber with a moment of pause and an excuse to leave the bank unobstructed, thus preventing a robbery.

## **THE PREVENTIVE APPROACH**

### ***Stopping the robber with customer service***

By analyzing bank robberies throughout the United States it was determined that they are overwhelmingly committed by a singular male subject. The individual enters the bank under the pretense of being a customer. These "customers" tend to only assume the "robber role" when a trigger point is reached. We have identified these trigger points to be singular contacts with bank employees or reaching a teller line and having singular contact with a bank employee.

Therefore, by eliminating these triggers, the would-be robber will most likely leave the bank without carrying his plan forward. To take full advantage of this discovery, the "SAFE" portion of the program facilitates this process in a step by step progression. The following is an explanation of the steps to be taken by bank employees:

#### **SCAN**

Scanning the work environment is the foundation of the SAFE portion of the program. Traditional security training for bank employees can cause a gap in this very important aspect of security. After training approximately 3,000 line employees, it was discovered a dual message was implied by past trainers, "don't be the hero, it's not your money, don't do anything, in fact if you do something other than nothing you could be fired." Then in the next breath employees were told be good witnesses.

The challenge now becomes getting employees to realize there are safe and effective actions they can take to prevent their victimization. To do this, they have to first become aware of a problem before they can take action. The following is an excerpt from the SAFECATCH training handout for tellers:

**S = Scan:        Scan your work area looking for suspicious persons or incidents.**

**DON'T SUPPRESS "THE GIFT OF FEAR":** "The gift of fear" (a term used by noted author, Gavin de Becker) is something

that we are all born with it. But from an early age on, we are often influenced by various factors to ignore it.

**CUSTOMER QUEUE:** In one robbery, the "Uncle Fester Bandit" stood in a teller line for five minutes. When interviewed after the robbery, the Victim Teller said that as soon as she looked up and saw him standing at her window, she immediately recognized him from alerts as the "Uncle Fester Bandit." Had she scanned the queue, she possibly would have seen him waiting in line, recognized him, and then utilized other strategies outlined below to avoid being robbed.

**EXTENDING YOUR "STRANGER DANGER ZONE:"** Just as important as being aware of what is happening inside your branch is being aware of what is happening outside of it.

For example, a team of take-over bandits had hit the same branch twice before. On their third attempt, an aware branch employee saw them exiting their vehicle and putting on masks. She could have just thought to herself, "*That's strange.*" Instead, she immediately yelled out "*They're back and are going to rob us again!*" The other branch employees immediately locked the entry door. The bandits approached and, upon finding it locked, turned and fled. They were apprehended a short time later.

### **ALERT**

Once a suspicious customer is identified, bank employees must be empowered to take action. Many times bank employees are aware of suspicious activity long before they are victimized. Employee feedback revealed they remained silent for fear of being wrong and possibly offending a customer.

The ALERT step of the program attempts to take that fear away. SafeCatch philosophy dictates that suspicious customers are treated the same as customers with which an employee would want to develop a business relationship. By doing this, SafeCatch becomes a customer development program with a bank robbery suppression nexus.

During the ALERT phase the bank employee is provided with their first preventative tool, the "walk-away" strategy. This strategy eliminates a trigger point by removing the teller from the line. It is used when the teller perceives the "Gift of Fear" and there is no time to take other action. It was developed from examples of failed bank robberies in Seattle's International District.

Due to a language barrier, it was found that when tellers in the International District were presented a demand note they often could not understand it. Because of this, they would excuse themselves from the "note-passer" seeking help from management. In all cases, when the teller walked away from the line the robber would leave the branch without completing his attempt.

To safely implement this tactic, tellers are trained that if they perceive the "Gift of Fear" and no demand has been made and/or a weapon displayed, they are to politely excuse themselves and walk away to a predetermined point of contact or alert another teller.

This has proven to be every effective in preventing several Seattle area robberies in the last three years. As with all aspects of the SAFECATCH program, if the subject (at anytime) makes a demand or displays a weapon, employees are trained to comply and move to the "CATCH" phase. The following is an excerpt from the SAFECATCH training handout for tellers:

**A = Alert:**        *Alert others to your suspicions. If the threat is immediate, utilize the "walk-away strategy" as described below.*

**"WHAT IF I'M WRONG?"**    The beauty of SAFE CATCH is that you are never wrong! Even when think you *may* be wrong, you're right. How can that be?

Because we are going to treat subjects that present to us the gift of fear exactly like we would treat a customer with whom we want to develop a banking relationship.

### **"LEGITIMATE NEEDS" VERSUS "CRIMINAL INTENT"**

A legitimate customer's thoughts:

- *'My business really matters to this bank!'*
- *'I'm being provided prompt, personal attention.'*
- *'I'm being provided information about banking services.'*

A would-be bandit's thoughts:

- Anxiety: *'I think they know why I'm here.'*
- Paranoia: *'I bet they've already called the police on me.'*
- Fear of capture: *'If I don't get out of here fast, I'm going to go to jail.'*

**"WALK-AWAY STRATEGY":** If a perceived threat is imminent, no weapon has been displayed, and/or no verbal or written demand has been made, walk away to your pre-determined point-of-contact, which is another branch employee.

For example, the teller would call out to the subject, "I'm having a computer problem. I'll be right back." Then, the teller should walk away to the pre-determined point-of-contact and alert that employee to their suspicions.

Then, the pre-determined point-of-contact can use the next SAFE CATCH step, "Friendly."

**DEMAND MADE/WEAPON DISPLAYED:** Once again, the above "walk-away strategy" is to be used only prior to a demand being made and/or a weapon being displayed.

**If a subject has made the robbery demand or has displayed a weapon, do not walk away.** Simply comply with the demand and then move on to the steps of "CATCH" as outlined in that section.=

### **FRIENDLY**

The FRIENDLY portion of the program is the next preventive tool provided and is based in part on traditional business greeting standards. Specifically, employees are trained to approach suspicious customers and state, "Hi, welcome to the bank, I don't recognize you as a customer, Are you here to open an account with us?"

The words are important because it opens two avenues, one customer service the other prevention. This statement also strips the potential robber of his ability to stay anonymous. After the greeting, the subject most likely will state his business, at which time the employee moves to the next step. The following is an excerpt from the SAFECATCH training handout for tellers:

**F = FRIENDLY: By being friendly, we take control and keep the subject in his "role."**

When a would-be note job bandit enters your branch, he "assumes the role" of one of your customers. He must maintain this "role" all of the way up to the teller window. Only then does he assume a new role, that of a bank robber.

By overtly treating him as a customer well before that point, there is a strong possibility that you will be able to keep him

in that customer "role" thus never allowing him to assume the role of a robber.

For example, you may approach the subject in a friendly manner and say: *"Hi, my name is (so-and-so). I'm the (your position) here. I don't recognize you as one of our customers. You must be here to open a new account."*

Remember, it's friendly, friendly, friendly. You're not looking to cause an escalation by your manner of approach; you're just looking to take away the subject's guise of anonymity or invisibility by approaching him in a warm, friendly manner just like you do with all of your customers.

Then immediately proceed to the next step, "EXIT."

### **EXIT**

After the greeting, employees are trained to immediately break contact and walk towards a desk or other alternate location separate from the teller line. Upon doing so state, "I can help you with that over here, I just need to see your ID."

If the contacted individual is a legitimate customer, this will be a great opportunity to build a relationship. If the subject is in the branch for illegitimate reason's he will likely pat his pockets and state, "I left my ID in the car" and walk out of the branch. Again, if the subject makes a demand when greeted, employees are trained to comply and move to the CATCH phase. The following is an excerpt from the SAFECATCH training handout for tellers:

**E = EXIT:** *Immediately after the greeting, provide an opportunity for the subject to exit.*

**BUILD YOUR BUFFER:** Immediately after saying "...You must be here to open a new account," the point-of-contact employee breaks contact and begins walking away from the subject back to their desk while saying, "I will just need to first see some photo I.D. and then I can help you right over here."

**"NO PENALTY FOR EARLY WITHDRAWAL:"** The subject, having had his anonymity taken away and having been provided a ready-made excuse, will most likely pat his pockets and state, "Oh, I forgot my I.D. in the car. I'll be right back." Then he will turn around, and leave.

**REPORT SUSPICIONS TO 911:** If the subject entered in the role of a customer and was provided the above level of customer service and yet left without conducting normal business, he most likely was there to commit a crime. Therefore, call 911 to report suspicious activity. Then notify the appropriate individuals in your organization.

## **A NEW PARTNERSHIP**

*Stop the robber before he can get started*

### **CATCH**

Many times, no matter how alert or what methods are used, the robbery will not be prevented. Either the note-passer gave no signals of his intent or perhaps a take-over style robbery occurred where SafeCatch strategies are not applicable. No matter the nature of the robbery, the CATCH phase of the program applies in all situations. The CATCH phase provides bank employees with procedures geared towards a partnership with law enforcement.

This partnership increases the probability the robber may be caught by a police response or through viable investigative leads. Both capture methods, the police response or through viable leads will dramatically reduce the amount of robberies in a given area. This is because it will limit how many bank robberies an individual is able to commit before being caught.

### **Call**

From employee feedback it was learned that when tellers activated their alarms they believed they had activated the 911 system. Meaning they believed they had called law enforcement. Even though it is standard bank policy for employees to call 911 post-robbery, it is not being done because of the teller's belief they had already done so.

This industry standard is causing significant delays in reporting. By analyzing bank surveillance video and comparing that to law enforcement dispatch logs it is not uncommon for reporting delays of up to five and ten minutes. When factoring in law enforcement response times, arrivals on-scene are not occurring until 10 to 15 minutes after the event. This built in delay is ensuring the robber's escape and ability to commit future robberies. To combat this, line employees must be retrained to call 911. The following is an excerpt from the SafeCatch training handout for tellers:

**C = Call:        Call 911 as soon as possible!**

**"YOU CALL, THEY HAUL!"**

**If you're the victim, you make the call to 911.** Having another employee do so delays law enforcement in pursuing the suspect. That's because in virtually every case the victim teller is the only one with the details that responding officers need. **This is a situation where seconds count!**

**"THE ALARMING TRUTH ABOUT THAT BUTTON:"** DO NOT RELY ON YOUR ALARM BUTTON TO NOTIFY 911. Your alarm button does not initiate the 911 system as rapidly as your picking up the phone and calling 911 does. **Your alarm button is part of your corporate notification system; 911 is our emergency response system.**

Remember, the sooner that 911 is called after the suspect's exit, the faster the police can be on the trail to track down and capture the suspect, thus preventing more robberies and more victims.

**"HELP ME HELP YOU:"** As soon as the bandit's hands hit the exit door or as soon as you feel safe to do so, pick up the phone and call 911. THEN, waive your hand to signal your coworkers that you have been robbed.

**DO NOT LEAVE YOUR TELLER STATION SEEKING APPROVAL TO MAKE THIS CALL. UPON COMPLETION OF THIS SAFECATCH TRAINING, YOU ARE HEREBY EMPOWERED AND EXPECTED TO PROACTIVELY PARTNER WITH LAW ENFORCEMENT TO CALL 911 IF YOU HAVE BEEN ROBBED.**

**ACTION**

Internal post-robbery notification was also found to lead to further delays in the notification process. After a robbery the victim teller leaves her work station seeking the manager. Once she has explained the robbery to the manager, action is taken; employees and customers are briefed, often individually. By now any opportunity for meaningful efforts by bank employees to assist in the investigation have long passed.

To overcome this, employees need to be trained that when they observe another employee on the phone with their hand in the air, they are to point at the teller and confirm the robbery. Once a robbery has been confirmed the employee is to announce to the branch in a clear calm voice, "The bank has been robbed, the robber is gone, we're all safe." This not only conveys the needed information in seconds, it sets up the next step in the "CATCH" phase. The following is an excerpt from the SafeCatch training handout for tellers:

**A = Action: If you see a co-worker on the phone with their hand in the air, take action. Lock the doors and notify management.**

You, as the non-victim employee, should simply ask the Victim Teller, "**Have you been robbed?**" If the Victim Teller gives you a positive response (in some manner) while talking to 911, you are to yell out for all branch employees and customers to hear, "**We were just robbed but we're safe! Again, we were just robbed but we're safe!**"

By doing this it allows for rapid notification to all other branch employees so that all can move on to the next step, "Tactical."

## **TACTICAL**

Typically, leads developed post robbery come from customers in the bank's parking lot. They are sitting in their vehicle's completing paperwork prior to entering the branch and see something suspicious. This phase moves some of that responsibility to the employees. When they hear an alert, they respond within seconds to a tactical position within the branch so they can view fleeing subjects and vehicles. The following is an excerpt from the SAFECATCH training handout for tellers:

**T = Tactical:** *When notified a robbery has occurred, go to your predetermined tactical location to observe fleeing subjects or vehicles.*

### **"WHICH WAY DID HE GO, WHICH WAY DID HE GO?"**

As a team, **choreograph and rehearse** who will go to which window on which side of the branch after the bandit has fled.

**"HE WENT THAT-AWAY!"** Try to ascertain a description of the getaway vehicle and the direction of travel so that this can be relayed to the Victim Teller who can, in turn, relay it to 911.

## **NEVER FOLLOW SUSPECTS OUTSIDE OF THE BUILDING!**

## **CASH**

From interviewing bank robbers, it has been discovered they choose their victim banks based on a varied set of criteria, one being how much money they receive during the course of a robbery. If the robber obtains cash above an average amount of \$1,000 to \$2,000, there is a strong likelihood the robber will return to the same branch or begin targeting a particular bank's branches. They do so based on the belief that this particular bank has more money in their drawers or policies that allow for a bigger take.

To combat this, tellers should be trained to comply with a robber's demands but attempt to limit the amount of money given. They do this by disguising the money given as a larger sum by removing a stack of fives and tens from

their drawer and placing one, one hundred dollar bill on top of the stack. This technique is analogous to handing out a device and should be thought of as such. If a robber, seeing this, asks for more money the employee complies without resistance. The following is an excerpt from the SAFECATCH training handout for tellers:

**C = Cash: Limit the amount that goes out and limit the robber's clout.**

**REHEARSE TAKING OUT DEMAND MONEY:** Go through the motion so that in a real-life robbery you will limit the amount you give out. That's because FBI statistics show that bandits often return to rob banks where in a previous robbery they got a lot of money. Rehearse grabbing your ones, your fives, your tens, your device, and then slapping just ONE \$100 bill on top and giving this to the suspect.

Once you've given the bandit the demand money, close your drawer and take a step back away from your drawer.

If the suspect demands more money, then you should comply.

If he walks away with less cash than he usually gets, he will most likely not come back to your branch or bank.

**REHEARSE PASSING YOUR DEVICE:** Visualize and practice handing out your security device (i.e. dye pack, tracking device, etc.)

**REGULAR MAINTENANCE OF SECURITY DEVICES:** Know the operation and maintenance requirements of all security devices (i.e. cameras, dye packs, tracking devices, etc.) Immediately contact the appropriate department if there were any questions or problems with any of the security equipment, or to arrange training on the operation and maintenance of any security devices.

## HELP

There appears to be a standard mind set within the banking industry that since certain institutions rarely suffer a robbery, then those institutions don't feel the need to put resources towards the issue. For the SafeCatch program to achieve its desired results the banking community as a whole need's to adopt the program. The final step in the program is an attempt to get the banking industry to understand that **every bank robbery is every bank's problem**. The following is an excerpt from the SAFECATCH training handout for tellers:

**H = Help:** *Help reduce bank robberies by committing to the proactive approach and partnership of "SAFECATCH."*

**PROACTIVE PARTNERSHIP:** By doing this, we will shift from *merely reporting* a crime to proactively partnering with law enforcement to prevent more bank robberies and to aid in the capture of bank robbery suspects.

## **SPECIAL CONSIDERATIONS**

In developing the SafeCatch program several long held industry standards were identified which could potentially be harmful to a positive resolution of bank robbery incidents. As such, it is suggested that financial institutions adopt the following changes.

### **ISOLATING THE VICTIM TELLER AFTER THE ROBBERY**

#### ***Current procedure and history***

Current industry standard dictates that the victim teller is isolated after the robbery and awaits law enforcement's arrival. Traditional thought dictates that keeping the victim teller isolated from other employees will keep clear and untainted the recall of the robber's description. In the pre-DVR era, it could take days for the 35mm film to be developed, this policy was actually useful. But by the mid 90's most banks were able to record images and today most have digital capability. Many times images are available when officers arrive at the branch which virtually eliminates the need for teller recall.

#### **PROPOSED CHANGE**

Do not isolate the victim teller, she is generally the only person who has the information needed by law enforcement. Instead the victim teller should be instantly engaged with law enforcement via 911 until their arrival on-scene.

#### **EXPECTED BENEFIT**

By not isolating the victim teller, a better working environment is created as the victim is in control of her safety and well being. By empowering employees to take direct action after their victimization they maintain that control which can diminish the effect of being victimized. This also allows (most important for law enforcement purposes) for a real time conduit of information to law enforcement and branch staff, resulting in a better police response to the robbery.

## **COMPLETING ROBBERY SUSPECT DESCRIPTION SHEETS**

### ***Current procedure and history***

Currently, most banks have implemented the law enforcement driven policy to have everyone who witnesses the robbery (Victim Teller, other employees, and customers) complete a "Robbery Suspect Description Sheet" while awaiting the arrival of law enforcement. In the heyday of 35mm cameras, when downloading images (if even available) took days, such sheets were tremendous aids to law enforcement. Now, with the advance of digital camera systems, images are almost immediately available.

Most of the time the information provided on such sheets is conflicting, not only with the recorded image, but with the sheets completed by other employees and customers. This brings about the possibility of creating distortions in the investigative process and exculpatory opportunities detrimental to successful prosecutions.

### **PROPOSED CHANGE**

Discontinue the use of "Robbery Suspect Description Sheets" for DVR-equipped branches. With SafeCatch, bank employees contact 911 directly and assumed their predetermined tactical positions. This will translate into faster response times by law enforcement and employees being engaged in productive activity until their arrival. This will leave little to time to complete the form.

### **EXPECTED BENEFIT**

By urging banks to stop using these forms we eliminate, or greatly reduce the chance, of creating confusing or misleading information which could lead to investigative or prosecutorial difficulties. If the investigation and prosecution proceed in an efficient and productive manner, it will lead to quicker apprehensions, longer jail sentences which thereby creates' a drop in robberies.

## **LOWERING THE EXIT CAMERA TO SIX FEET**

### ***Current procedure and history***

A survey of bank camera surveillance systems throughout the industry reveals that they are placed too high (well above 7'). Most bank cameras were mounted high up on walls, or mounted from high ceilings, so as to be nearly unnoticeable.

Due to the prevailing social norms of the day during the 1970's, most hat-wearing males removed them upon entering a building, leaving the face exposed. However, today's changing social norms now allow for the wearing of baseball caps inside buildings and its commonplace. Hence, high-mounted surveillance camera systems costing thousands of dollars can be defeated by wearing a baseball cap.

### **PROPOSED CHANGE**

Re-position cameras (even just one is adequate) so that they obtain full, frontal face shots of baseball cap-wearing suspects. If due to cost or decor only one camera can be adjusted, it should be a camera that captures the suspect's face as he exits. A review of bank surveillance film reveals that as most suspects exit a branch, they often raise their head believing they are making a successful, "photo-free" escape.

### **EXPECTED BENEFIT**

The key to quick resolution is identifying the robber as quickly as possible. By encouraging banks to lower their exit cameras so as to provide an image of investigative quality (images that have facial features visible) it will put an end to a robbery spree before it essentially gets started. Again, a quicker identification leads to a quicker arrest, thus reducing the number of banks robbed by a particular suspect.

Additionally, photos that reveal facial features are far more valuable as evidence for prosecution. Many times, quality surveillance photos lead to plea deals. These pleas save thousands of dollars for both financial institutions and the court system, not to mention the strain on bank employees from not having to testify.