

**CREDIT CARD ACCOUNTABILITY RESPONSIBILITY  
AND DISCLOSURE ACT OF 2009**

**REPORT ON EMERGENCY TECHNOLOGY FOR USE WITH ATMs**

**April 2010**

**Submitted by:  
Bureau of Economics  
Federal Trade Commission**



## **Executive Summary**

Every year millions of transactions are conducted using the nation's estimated 400,000 automated teller machines ("ATMs"). Before, during, or after withdrawing cash from an ATM, a customer may be the target of a robbery or other violent offense. The Credit Card Accountability Responsibility and Disclosure Act of 2009 (the "Act") mandates that the Federal Trade Commission ("FTC") provide an analysis of any technology, either currently available or under development, which would allow a distressed ATM user to send an electronic alert to a law enforcement agency. In particular, the FTC was directed to evaluate the efficacy of so-called "emergency-PIN" and "alarm button" technologies by: (1) providing an estimate of the number and severity of any crimes that could be prevented by the availability of these devices; (2) estimating the costs of implementing such devices; and (3) comparing the costs and benefits of at least three types of such devices. Although FTC staff determined that the requisite data to evaluate the efficacy of these technologies are not available, staff nevertheless conducted a review based on other materials to provide a sense of the value of the technology.

FTC staff reviewed various ATM trade press reports and academic studies and contacted a range of entities – several government agencies, a number of major, private financial institutions, other firms, trade associations involved with ATMs and ATM

## **I. Study Required Under the Credit Card Act of 2009**

Section 508 of the Credit Card Accountability Responsibility and Disclosure Act of 2009 (“the Act”)<sup>1</sup> mandates that the Federal Trade Commission (“FTC” or “Commission”) conduct a study (hereafter “the study”) on “the cost-effectiveness of making available at automated teller machines [“ATMs”] technology that enables a consumer that is under duress to electronically alert a local law enforcement agency that an incident is taking place at such [ATM] . . . .”<sup>2</sup>

The Act specifies two such technologies to be evaluated:

“an emergency personal identification number that would summon a local law enforcement officer to an [ATM] when entered into such [ATM] . . . .”<sup>3</sup>

“a mechanism on the exterior of an [ATM] that, when pressed, would summon a local law enforcement [officer] to such [ATM].”<sup>4</sup>

The first security measure is commonly referred to as “reverse-PIN” or “emergency-PIN” technology and the second as “alarm button” technology.

Under the Act, the study should include: (1) “an analysis of any technology [allowing a distressed ATM user to electronically contact a law enforcement agency] that is currently available or under development”; (2) “an estimate of the number and severity of any crimes that could be prevented by the availability of such technology”; (3) “the estimated costs of implementing such technology”; and (4) “a comparison of the costs and benefits of not fewer than 3 types of such technology.”<sup>5</sup> The Commission is to issue

---

<sup>1</sup> Credit CARD Act of 2009, Pub. L. 111-24, § 508.

<sup>2</sup>

a report of the findings of the study no more than nine months after the date of the



alarm button system, or to infer the effects of such a system from any similar technology employed at ATMs.

Second, neither the DOJ, the Secret Service, nor the FDIC track data on the specific security devices installed at individual ATM locations or specify ATM crimes where the victim is “under duress” during an ATM withdrawal. Thus, these government agencies do not have reliable data on the amount of crime that an emergency-PIN or alarm button system might affect. The Secret Service and FDIC both track some data on the incidence of ATM *fraud* offenses, which would not be deterred by emergency-PIN or alarm button technology.<sup>8</sup>

Some of the respondent banks appear to track information on the security devices and crimes committed at their ATMs. According to one of these banks, ATM

larceny. Most of these crimes are burglaries, which are offenses against property or “property crimes,” as opposed to crimes against persons, which are also referred to as “violent crimes.” ATM robbery, which is a violent crime, is the only offense category in the BCS data that emergency-PIN or alarm button technologies might be expected to affect.

Most of the ATM robberies captured in the BCS data involve traditional bank robberies in which the offender had a bank employee remove money from an ATM located at the banking site during the course of the robbery.<sup>10</sup> BCS data do not capture robberies committed while a bank customer attempts to withdraw funds from an ATM because those robberies are not federal offenses.<sup>11</sup> As a result, the FBI’s BCS data do not provide a credible estimate of the number or severity of ATM crimes committed involving bank customers, and thus they do not provide an estimate of ATM crimes that could be deterred by ATM security devices.<sup>12</sup>

### **C. Data from Local Law Enforcement Agencies**

FTC staff also sought ATM crime data from local law enforcement agencies. While some police agencies apparently have begun to track more carefully crimes involving the use of ATMs, these data do not appear to be useful for the purpose of

---

<sup>10</sup> E-mail from Bradley V. Bryant, Unit Chief,





#### **D. Data from Trade Associations and Businesses**

The staff contacted two trade associations affiliated with the ATM industry, a manufacturer of ATMs and provider of ATM security solutions, and three holders of patented ATM technologies, including two emergency-PIN providers and one alarm button provider. None of these entities was able to provide sufficiently detailed data on ATM crimes for use in the study.

FTC staff also contacted several of the largest banks in the U.S. to determine any data they might have for the study. Staff sent detailed questionnaires to five major banks regarding the tracking of ATM offenses, the security devices installed at ATMs, and the costs of implementing an emergency-PIN or alarm button system. Three banks responded to the FTC inquiries.<sup>17</sup> However, these banks indicated that they did not have sufficient data for the study.

---

<sup>17</sup> The FTC staff's data collection efforts were conducted within the parameters of the Paperwork Reduction Act 44 U.S.C. §§ 3501 *et seq.*, which limits the staff's ability to obtain the same information from more than nine separate entities. The FTC staff identified the specific banks to be contacted from a list of the largest bank holding companies maintained by the U.S. Federal Reserve System. *See* <http://www.ffiec.gov/nicpubweb/nicweb/Top50Form.aspx>. When responses were not received, staff placed phone calls or e-mails with the next largest company down on the aforementioned list. The three responses that staff received come from the first, second, and fourth largest banks in the U.S. in terms of total assets, *id.*, and are thus likely to ac-.008(w[( of)3sshe U.



An ATM reverse-PIN system called “SafetyPIN” was invented by Joseph Zingher and patented in March 1998.<sup>20</sup> According to Mr. Zingher, SafetyPIN is a simple computer code “that would recognize reversed, inverted, or otherwise altered [PINs] as a distress signal, and [instruct] the teller machine to call the cops.”<sup>21</sup> The electronic message relayed to an alarm company dispatcher would contain “the card holder’s name, identifier and location. (The identifier is usually their driver’s license, date of birth + full name, etc).”<sup>22</sup> For several years, Mr. Zingher attempted to sell SafetyPIN to banks in Illinois, Georgia, and Florida, but his attempts were unsuccessful.<sup>23</sup> Mr. Zingher offered to make the product available for free on a trial basis to banks in Kansas, but his offer was declined.<sup>24</sup> Mr. Zingher reports that he has had no customers for his emergency-PIN system and that he is unaware of any other emergency-PIN system in use.

---

<sup>20</sup> Computerized System for Discreet Identification of Duress Transaction and/or Duress Access, U.S. Patent No. 5,731,575 (filed April 21, 1997) (issued March 24, 1998) (*Zingher Patent*). Mr. Zingher markets SafetyPIN through his company Zi Cubed, of which he is both the sole proprietor and employee. See <http://www.zicubedatm.com/>.

<sup>21</sup> Forbes: Banking on ATM Safety (January 28, 2004), available at <http://www.msnbc.msn.com/id/4086277>. The idea of a “duress code” associated with ATM customer PINs had actually been around for some time before Zingher’s patent. For example, on July 30, 1986, Representative Mario Biaggi, a former police officer, proposed that ATMs should employ such a code (US Congressional Record at 18232 *et seq.*). In 1987, Representative Biaggi proposed HR 785, which would have had the FBI evaluate the idea of an emergency PIN system (the resolution was not debated or voted out of committee).

<sup>22</sup> Letter from Joseph Zingher to FTC staff (November 30, 2009) (*Zingher Letter*).

<sup>23</sup> Forbes: Banking on ATM Safety, *supra* note 21.

<sup>24</sup> *Id.*

Another emergency-PIN system currently marketed to banks is “ATMOnGuard.”<sup>25</sup> This device, which Mr. Zingher identified as a competing product,<sup>26</sup> does not require a distressed customer to enter a reverse-PIN, but rather to hit a single keypad number (i.e., 0 through 9) after the customer’s PIN was entered. The additional single keypad entry would indicate whether the transaction was “normal” or being conducted “under duress,” which would subsequently send an electronic distress call to a dispatch center.<sup>27</sup> The ATMOnGuard system has never been deployed at any ATMs in the U.S.<sup>28</sup>

The respondent banks reported that none of their ATMs currently have installed, or have ever had installed, an emergency-PIN system of any sort. The ATM manufacturer Diebold confirms that, to its knowledge, no ATMs have or have had an emergency-PIN system.<sup>29</sup>

Some states have considered legislatively mandating banks to adopt a reverse-PIN system. In January 2004, Illinois considered a bill that would have required banks and other ATM providers to install reverse-PIN capabilities.<sup>30</sup> However, before enactment, the bill was amended to make the use6.55 0 TD.0003 Tc-.3shav”

remains alive in Illinois; last year, Illinois State Senator Jacqueline Collins introduced a bill in the Illinois Senate that would require that ATMs be fitted with reverse-PIN systems.<sup>32</sup> At present, this legislation remains in committee.

In 2004, a bill was introduced before the Kansas State Senate Financial Institutions and Insurance Committee that would have mandated the implementation of reverse-PIN technology at ATMs located in the state.<sup>33</sup> This bill was not enacted. In 2006, the Georgia State Assembly considered a measure that would have adopted reverse-PIN systems on ATMs.<sup>34</sup> This proposed legislation also was not enacted.

#### **B. Likelihood of Decreased ATM-Related Crime or Injury**

Despite the unavailability of the data that would be necessary to conduct the study mandated by the Act, the preponderance of the extant anecdotal evidence suggests that emergency-PIN technologies likely would not have a large impact on ATM crime. First, the best available evidence suggests that non-fraud ATM crimes in general occur with low incidence. Second, distressed ATM customers may not have the ability or incentive

---

personal identification number in reverse order, the terminal automatically sends an alarm to the local law enforcement agency having jurisdiction over the terminal location. The Commissioner shall promulgate rules necessary for the implementation of this subsection . . . .”); Public Act 93-0898 (eff. 8-10-04) (“The provisions of this subsection . . . shall *not* be construed *to require* an owner or operator of a terminal to design and program the terminal to accept a personal identification number in reverse order.”) (emphasis added). The relevant provisions of the two acts are codified at 205 ILCS 616, Section 50(i).

<sup>32</sup> See S.B.1355, 96<sup>th</sup> Gen. Assem., Reg. Sess. (Ill. 2009). The synopsis of the bill reads: “Amends the Electronic Fund Transfer Act. Provides that a terminal operated in the State must (instead of may) be designed and programmed so that when a consumer enters his or her personal identification number in reverse order, the terminal automatically sends an alarm to the local law enforcement agency having jurisdiction over the terminal location. Deletes language providing that specified provisions shall not be construed to require an owner or operator of a terminal to design and program the terminal to accept a personal identification number in reverse order . . . .”

<sup>33</sup> S.B. 333, 2004 Leg., Reg. Sess. (Kan. 2004).

<sup>34</sup> See S.B. 379, 148<sup>th</sup> Gen. Assem., Reg. Sess. (Ga. 2006).

to activate an emergency-PIN or alarm button device, and in some instances doing so might elevate the risk of harm to the customer. Third, police response times may not be fast enough to create a high probability that the offender will be apprehended, thereby limiting the deterrence effect of such measures with respect to ATM crimes. And fourth, offenders may simply change their practices in order to circumvent any additional risk posed to them from the deployment of emergency-PIN technologies.

### **1. Frequency of Crimes Susceptible to Emergency-PIN Use**

One crucial aspect of the effect of emergency technologies on crime is the frequency of crimes that may be susceptible to interruption or deterrence through the use of the technology. The little data available indicates that crimes that may be affected by the availability of an emergency-PIN system may not be common. Some academic research indicates that the majority of ATM robberies do in fact occur only after the victim has already withdrawn funds, which would prevent the user's activation of an emergency-PIN device located at the ATM while still under duress.<sup>35</sup> Some government investigations have concluded that ATM crimes are relatively rare occurrences, even though there do not exist any definitive data on the frequency of ATM crimes. For example, the Office of Banks and Real Estate of the State of Illinois concluded that:

Although there is no precise data on ATM crime, violent crime against ATM users is relatively rare. Over the decade of the 1990s, ATM crime has actually

---

<sup>35</sup> See Michael S. Scott, *Robbery at Automated Teller Machines*, U.S. Department of Justice, Office of Community Oriented Policing Services, Problem-Specific Guide Series No. 8 (2001), at 5 (citing W. Wipprecht, *Strike Back at ATM Crime* 25 JOURNAL OF CALIFORNIA LAW ENFORCEMENT 53 (1991) and R. Wright and S. Decker, ARMED ROBBERIES IN ACTION:e80.7S91)

decreased from approximately one crime per one million ATM transactions to one crime per 3.5 million transactions.<sup>36</sup>

In addition, as discussed above, many kinds of crimes often described as ATM crimes would not be affected by use of the technology.<sup>37</sup>

## **2. Distressed Customer Responses**

Critics of emergency-PIN security devices argue that distressed customers are unlikely to have the composure to remember and activate their PIN number in reverse sequence or activate some other emergency-PIN system, such as the ATMOnGuard solution.<sup>38</sup> Indeed, with regard to SafetyPIN, some commenters have argued that it is

---

<sup>36</sup> State of Illinois, Office of Banks and Real Estate, *ATM Report*, available at <http://www.obre.state.il.us/Agency/news/atmrpt.htm>, § I; see also Scott, *supra* note 35, at 2 (internal citations omitted):

As yet, there are no routinely collected national figures on the incidence of U.S.



probably challenging for most persons to instantaneously recall and recite their PIN backwards (assuming it is not palindromic) at will, much less when they are in physical danger.<sup>39</sup> For example, Bank of America reported:

It is unclear that the adoption of an ATM duress device would actually reduce crime at the ATM. For example, there are many challenges with the reverse-PIN solution. Our customers may have a PIN that is up to 12 digits in length.<sup>40</sup>

In its investigation of reverse-PIN technology, the Office of Banks and Real

Estate of the Illinois Department of Financial and Professional Regulation concluded:

[T]he reverse-PIN system attempts to utilize current technology to provide law enforcement with the immediate location and background information concerning a potential victim. However, a consumer may be under too much emotional stress to properly utilize the system . . . and no evidence exists that the reverse-PIN system would actually reduce crime.<sup>41</sup>

As such, the Office could only recommend further study into the efficacy of reverse-PIN technologies.<sup>42</sup>

---

kidnapping,” or a situation in which a criminal abducts a victim, forces him or her (or uses his or her card) to make forced withdraws at one or more ATMs, and then

### 3. Law Enforcement Response Times

Assuming that a distressed customer would be able and willing to activate his or her emergency-PIN, such measures would not be expected to deter crime unless they actually lead to interruption of the crime in progress, or at least to the identification and apprehension of offenders by local law enforcement authorities. A threshold question therefore is whether the police could respond quickly enough to a distress call to have a reasonable chance of making an arrest, and therefore potentially deter other potential criminals from engaging in ATM crimes. If police cannot respond quickly enough to interrupt the crime and apprehend the criminals, emergency-PIN systems are unlikely to deter ATM-related crime.<sup>43</sup>

An offender is unlikely to need to remain at the scene of the crime for very long after an ATM customer enters an emergency-PIN. However, DOJ-compiled data in 2006 indicate that 26.4 percent, or just over one-quarter, of police response times to reported robberies occurred within five minutes. Approximately 38.9 percent occurred within 6-10 minutes, and 15.5 percent occurred within 11 minutes to one hour.<sup>44</sup> Thus, in a majority of instances, police response times to violent robberies would exceed that necessary for interrupting the crime or apprehending the offender.<sup>45</sup> Nonetheless, responses within 5 minutes were not infrequent. Also, the potential for such a response

---

<sup>43</sup> If police are in fact slow to respond to such distress calls, then ATM users will have little incentive to even attempt to use them in the first place, an effect that is exacerbated if users recognize that they may “fumble” the attempt and increase their own danger.

<sup>44</sup> Bureau of Justice Statistics, Office of Justice Programs, U.S. Department of Justice, Criminal Victimization in the United States, 2006 Statistical Tables (2008), *available at* <http://bjs.ojp.usdoj.gov/content/pub/pdf/cvus06.pdf>, at tbl. 107.

<sup>45</sup> In addition, Mr. Zingher indicates that his system is expected to provide emergency signals to burglar-alarm companies rather than directly to law enforcement, which could add to the total response time after the reverse-PIN is used. *See Zingher Letter, supra* note 22.

time could be enough either to deter some crimes or to deter some criminals from remaining after obtaining the money to inflict physical injury on their victims. FTC staff found no basis for assessing the relative likelihoods of these response times deterring or not deterring crimes or physical injury.

Furthermore, some ATM crime victims never actually see their offender because they are approached from behind. Even if the police can get to the scene relatively quickly, victims may be able to provide the authorities only limited information about the physical characteristics of the offender.

#### **4. Potential Changes in Offenders' Practices**

To the extent that the presence of an emergency-PIN system at an ATM may deter robberies at that ATM, another issue is whether voluntary, localized installation of such a system would simply cause offenders to frequent other ATMs without the system. Further, even deployment of such systems at all ATMs in a relatively wide geographic region, such as in response to a legal mandate, might not have a significant impact on the incidence of ATM crimes. Such laws may limit the extent to which potential criminals may geographically displace their activities, but they might do little to mitigate any *temporal* displacement effects. For example, the installation of emergency-PIN systems at ATMs throughout a large metropolitan area may result in criminals adjusting their behaviors so as to confront the ATM customer only after he or she has already withdrawn funds.<sup>46</sup> Such adjustments in criminal behaviors, which seem relatively minor, could result in little or no decrease in the frequency of ATM crimes, though the latter

---

<sup>46</sup> This discussion assumes that potential criminals would be deterred in the first instance from confronting victims in the process of attempting to withdraw funds at ATMs with emergency-PIN systems, but, for the reasons discussed above, this assumption may not hold. *See supra* Section III.B.2.

adjustment could cause the average per offense amount of money stolen from the victim to fall.

The marketers of emergency-PIN technologies have focused on a subset of ATM crimes known as “express kidnappings” (als



Diebold Inc., a manufacturer of ATMs and provider of various ATM security solutions,<sup>51</sup> indicated that it has had numerous conversations with banking institutions regarding the implementation of an emergency- or reverse-PIN system.<sup>52</sup> None of those banks expressed any interest due to concerns that customers might increase their chances of harm if they fumbled entering their emergency-PIN numbers.<sup>53</sup> Diebold concurs with this sentiment and does not believe that implementing an emergency-PIN system is prudent.<sup>54</sup>

The report of the Illinois Office of Bank and Real Estate similarly notes:

The deterrent [effect] of having such a system in place is another touted feature of the [reverse PIN] system. However, deterrence does not prevent crime in progress. More importantly, the law enforcement community does not generally encourage resistance or confrontation to thwart theft or robbery. The risk of physical harm to the customer is greatly increased should they resist. When coupled with the fact that ATMs generally limit withdrawals to approximately \$200.00, engaging a criminal in an altercation or otherwise offering resistance over such an amount does not appear to be prudent.<sup>55</sup>

FTC staff found no evidence confirming this risk (note again that the technologies have never been employed), but staff also found neither evidence nor analysis disputing the risk.

**D. Costs of Implementation**

FTC staff could not reliably determine the costs of implementing an emergency-PIN technology, in part because such a techno

as well as for the central systems that run the ATM networks.<sup>58</sup> Other costs relate to: (1) additional investments in physical capital (e.g., installing a dedicated high-speed data transmission line between the ATM and the emergency dispatch center); (2) ongoing maintenance costs for the software and physical equipment and other recurring costs; and (3) licensing fees/royalties for the patented emergency-PIN system.<sup>59</sup>

Upgrades for the central systems might be needed to ensure interconnectability among all ATMs, regardless of network. For example, if a Bank of America account holder is held up while attempting to withdraw funds from a Citibank ATM, the Citibank ATM would have to be able to recognize the emergency-PIN associated with a Bank of America debit card in order to properly alert the local authorities. Wells Fargo noted: “For an alert mechanism to be effective, it would need to be consistently applied regardless of the ATM that was used (owned by the customer’s bank, another bank, or an independent operator, the card that was used, and the municipality in which the crime took place). This would require the coordination of literally *thousands* of [different] entities.”<sup>60</sup>



## 2. Potential Suppliers' Cost Estimates

The potential supplier of an available emergency-PIN system, Mr. Zingher, states that installing his SafetyPIN solution would cost approximately \$25 per ATM.<sup>61</sup> This figure is his estimate of the cost, expressed on a per-ATM basis, to upgrade the PIN verification subroutine on the various computers that run the nation's ATM networks to enable them to send out an electronic text message to the relevant alarm center.<sup>62</sup> Mr. Zingher's estimate implies that the total cost of upgrading the approximately 400,000 ATMs deployed across the U.S.<sup>63</sup> to use his emergency-PIN technology would be around \$10 million.

Mr. Zingher states that his system does not require software or other upgrades to the individual ATM machines. It is not clear whether Mr. Zingher's estimate reflects interconnection costs among the ATM networks that might be needed to implement an emergency-PIN system across the country. In particular, one of the features marketed with SafetyPIN is its ability to pull information from the distressed customer's driver's license record. This information is pulled at the time the distressed customer activates the technology, and it is relayed to law enforcement officers along with the electronic message indicating the customer's location. Making driver's license data available to the police may allow them to identify a victim who is transported during an express

---

<sup>61</sup> See, e.g., Final Report of the ATM Safety Study Committee, Senate Research Office, Georgia General Assembly (2006), at 6, available at [http://www.legis.state.ga.us/legis/2009\\_10/senate/publications/sro/committee\\_reports/2006/atm-safety-study-committee-report.pdf](http://www.legis.state.ga.us/legis/2009_10/senate/publications/sro/committee_reports/2006/atm-safety-study-committee-report.pdf).

<sup>62</sup> Zingher Interview, *supra* note 16; Zingher Letter, *supra* note 22.

<sup>63</sup> The estimated number of ATMs in the U.S. is taken from the Final Report, *supra* note 61, at 3; Zingher Interview, *supra* note 16.





PINs sent over the ATM network and ma

ACI Worldwide, a major provider of electronic payments software, including the software that runs the HSM,<sup>76</sup> stated that it had once started the process of conducting a formal cost study for implementing a reverse-PIN system in Illinois when the State considered requiring the system on ATMs.<sup>77</sup> The company never completed the cost study because the requirement was never enacted.<sup>78</sup> Hence, it could not provide FTC staff with any cost estimates. ACI Worldwide stated that an emergency-PIN system likely could be implemented solely through software modifications to the ATM network, but was uncertain if such modifications would be limited only to the software pertaining to the HSM.<sup>79</sup>

The State of Illinois ATM Report noted four significant “computer interface barriers” to an effective reverse-PIN system:<sup>80</sup>

First, are the limitations inherent in the use of PIN numbers. The system would double the amount of PINs used per person.<sup>81</sup>

Second, conversion to this system requires a significant commitment in resources to writing the new computer programs that recognize the reverse-PIN and then make multiple complex decisions. Currently, ATMs communicate with banks and make what are termed ‘binary’ (i.e., simple ‘yes/no’) decisions concerning the account and transaction information. Under the reverse-PIN system, the main computer must: (a) determine and communicate with the police station closest to the ATM; (b) the computer must communicate with the bank account of the cardholder and obtain account information that is usually confidential and protected (this process

---

<sup>76</sup> Interview with Richard A. Duval, Senior Strategic Alliance Manager, ACI Worldwide (March 3, 2010).

<sup>77</sup> *Id.*; see *supra* notes 31-32 and accompanying text for discussion on the history of reverse-PIN legislation in Illinois.

<sup>78</sup> Duval Interview, *supra* note 76.

<sup>79</sup> *Id.*

<sup>80</sup> See *ATM Report*, *supra* note 36, § III (“Computer interface problems are estimated to be significant and costly in implementing the reverse PIN system at this time.”).

<sup>81</sup> *Id.*

is more complicated if the ATM is not from the accountholder's bank);  
and, (c) the main computer must then also communicate with the Secretary

relevant data concerning the costs of deploying an emergency-PIN system. Neither of these entities was able to provide such information.<sup>87</sup>

**E. Summary**

Based on the above information and analyses, staff concludes that the costs of implementing an emergency-PIN system could be substantial, though it cannot gauge how substantial. Staff also concludes that there is currently no way to determine the extent of ATM-related crime subject to interruption or deterrence through such a system or the net effect of deploying such a system. While there may be some potential for decreasing ATM-related crime and injury, there is also the possibility that emergency-

caller, but he/she can also hear noises and conversations within twenty (20) feet of the ATM.<sup>88</sup>

ATM911 can be installed on either walk-up or drive-up ATMs<sup>89</sup> and does not require the customer to purchase a new ATM.<sup>90</sup>

SafeAlert Systems has sold alarm button systems for about 2,000 individual ATMs over the past 18 years.<sup>91</sup> If all these buttons were currently in use, that would represent approximately 0.5 percent of all ATMs in the U.S., assuming there are 400,000 ATMs in the U.S.<sup>92</sup> The company reported that some banks have chosen to uninstall the buttons, and for this reason it cannot provide an exact figure on the number of ATMs at which ATM911 is currently deployed. Furthermore, because the company no longer installs the systems itself, but instead works through third party “dealers” (often security system companies) who perform this function, it is unable to provide the number of bank entities that have purchased (or are currently using) the system.<sup>93</sup>

None of the ATMs of the respondent banks currently employ alarm button technology. One of the respondent banks, Wells Fargo, reported conducting a pilot program in the early 1990s with such alarm buttons on several ATMs in California. According to that bank, this program resulted in a large number of false alarms that led law enforcement officials to request the removal of the devices.<sup>94</sup>

---

<sup>88</sup> <http://www.safealert.com/How.shtml>.

<sup>89</sup> <http://www.safealert.com/ProductDescription.shtml>.

<sup>90</sup> Interview with Larry Steelman, Vice President, SafeAlert Systems (February 25, 2009).

<sup>91</sup> *Id.*

<sup>92</sup> *See supra* note 63.

<sup>93</sup> Steelman Interview, *supra* note 90.

<sup>94</sup> *Wells Fargo Letter*, *supra* note 50.



Several small cities have mandated the installation of alarm buttons along with surveillance cameras on all ATMs that operate within their jurisdictions. SafeAlert Systems informed FTC staff of three cities outside Cleveland, Ohio, that do so: Broadview Heights, Brooklyn, and Strongsville.<sup>95</sup> FTC staff also identified another small municipality that has mandated the adoption of ATM alarm buttons, the Sharon Hill Borough in Delaware County, Pennsylvania. The Borough's ordinance, which was passed in March 2006, required that alarm buttons and CCTV cameras be installed on all outdoor ATMs.<sup>96</sup> Only one of the ATMs in the Sharon Hill Borough is located outdoors, and it has an alarm button.<sup>97</sup>

SafeAlert Systems does not recommend that a distressed ATM user attempt to push the alarm button while a crime is in progress, as doing so could increase the probability that the offender will inflict physical harm.<sup>98</sup> Rather, SafeAlert Systems advises victimized ATM users to push the button in order to request assistance or to report the crime only after the offender has left the scene. ATM911 is not a technology specifically designed to enable a consumer that is under duress to electronically alert a local law enforcement agency that an incident is taking place, and thus is not a system that the Act mandates that the FTC study.

---

<sup>95</sup> See City of Broadview Heights, Ordinance No. 93-96 (approved July 23, 1996); City of Brooklyn, Ohio, Ordinance No. 1996-7 (adopted February 2, 1996); City of Strongsville, Ohio, Ordinance No. 1996-123 (approved July 1, 1996).

<sup>96</sup>

**B. Likelihood of Decreasing ATM-Related Crime or Injury**

As with emergency-PIN technology, alarm button systems do not address most kinds of ATM-related crimes, and existing data on ATM crimes do not distinguish between those that might have been halted or solved through use of an alarm button and those that would not. Further, as with emergency-PIN technologies, it is not clear whether police response times are fast enough to create a reasonable probability that law enforcement officers will be able interrupt the crime or make an arrest.

Wells Fargo described an alarm button pilot program it had conducted, which showed no positive effect over its duration:

In the early 1990s Wells Fargo conducted a pilot with the Oakland, California

is installed.<sup>102</sup> However, it was not aware of any formal studies that have evaluated the effect of the technology on crime.<sup>103</sup>

SafeAlert Systems provided FTC staff with letters supporting the adoption of ATM911 from officials of two of the Ohio cities. A letter from an official for the City of Brooklyn official stated that ATM911 “was enacted . . . for the purpose of protecting the users at [ATMs] in the City of Brooklyn . . . . Our City’s Chief of Police . . . feels that having these panic buttons are a great deterrent in fighting crime at [ATMs].”<sup>104</sup> This letter does not provide any data or indication on the extent to which ATM crime rates may have fallen as a result of ATM911 adoption. A letter from the Strongsville Police Department speaks to the issue of deterrence more directly, stating: “Before this ordinance was enacted there were two robberies at bank ATMs within Strongsville. After the ordinance there have been no more robberies.”<sup>105</sup>

Despite these two testimonials, however, the effect of the alarm button on ATM crime is unclear. First, as the City of Strongsville letter indicates, there were only two ATM crime incidents preceding the adoption of the ordinance. It would be inappropriate to infer any causal crime-reducing effects from deployment of the ATM911 system from such a small a number of events. Second, each city’s ordinance mandated installation of the ATM911 system concurrently with closed-circuit television (“CCTV”) cameras on all

---

<sup>102</sup> <http://www.safealert.com/How.shtml>.

<sup>103</sup> Steelman Interview, *supra* note 90. SafeAlert Systems indicated that one reason why no such studies have been conducted is because there are no reliable data on ATM crimes. *Id.*

<sup>104</sup> Letter from Kenneth E. Patton, Mayor, City of Brooklyn to New Jersey Assemblyman Neil Cohen (August 2004).

<sup>105</sup> Letter from Sergeant John Hall, Crime Prevention Specialist, Strongsville Police Department to Richard Aborn, The Camber Group (April 30, 1999).

ATMs. It is unclear that any deterrent effect stemming from the adoption of the ATM911 system could be determined separately from any deterrent effect effectuated by the installation of CCTV cameras at all ATMs that occurred at the same time.<sup>106</sup>

Third, as SafeAlert acknowledged, even if crimes are deterred at those locations where a visible alarm button is installed, criminals may simply respond by searching out and committing crimes at ATMs that do not have the button present.<sup>107</sup> To the extent that criminals simply “geographically displace” the locations at which they commit their crimes in response to the deployment of ATM security technologies at specific sites, *overall* ATM crime rates may not be substantively affected.<sup>108</sup> In addition, widespread deployment of alarm button systems at all ATMs over a broad geographic area could result in “temporal displacement,”<sup>109</sup> where a criminal approaches an ATM customer after the withdrawal is complete and the customer is no longer close enough to the ATM to press a button. It is not clear to what extent criminals may have adjusted their behavior in such ways.<sup>110</sup> Because police reports and records may not detail the fact that a robbery

took place at or in the vicinity of an ATM, a reported ATM robbery in an area with alarm buttons may get officially recorded as an “ordinary” robbery rather than as an ATM robbery.

An assessment of the likelihood of actual reduction in crime or injury should take into account customers’ abilities to activate the system and the results of activation.<sup>111</sup>

While an alarm button system does not create the kind of difficulty for a distressed victim to remember an altered PIN number under duress, an alarm button’s use is not invisible to the robber, who may be able simply to prevent the victim from pressing the button through threats or force. In addition, the potential effects of law enforcement response times may be varied and the available information provides no basis for gauging their relative likelihood.<sup>112</sup>

### **C. Costs of Use**

#### **1. Increased Physical Danger**

As with emergency-PIN use, attempts to use an alarm button during a robbery might increase the risk of physical danger to

discourages efforts to resist robberies due to heightened risk of physical injury, and the manufacturer of the alarm button system, SafeAlert, itself cautions that the button should not be pressed during a robbery or until the offender has left the scene. Yet the visible presence of the button may encourage a distressed customer to press it as soon as possible, thus incurring that additional risk of harm.

## **2. False Alarms**

False alarms are an unintended consequence associated with alarm button technologies. Banks cite the frequent occurrence of so-called “false alarms” as one of the major shortcomings associated with these devices. Wells Fargo’s alarm button pilot program produced 500 false alarms and no legitimate ones.<sup>113</sup> Wells Fargo did not provide further detail on the circumstances underlying the 500 false alarm instances, but they may have included accidental pressing of the button, pranks, and overly nervous ATM patrons who believed they were under threat but actually were not. If police must routinely respond to these false alarms, fewer resources will be available for deterring or solving real crimes, which is another potential cost of alarm button technology.

SafeAlert Systems was the supplier of the alarm button devices used in the Wells Fargo pilot program.<sup>114</sup> The company claimed that Wells Fargo would not share specific information regarding the nature of the false alarms after the pilot program was terminated.<sup>115</sup> Although SafeAlert Systems subsequently modified the ATM911 system so that the alarm button could only be activated by the insertion of an ATM customer’s card, Wells Fargo was not interested in readopting the technology. The card-activation

---

<sup>113</sup> *Wells Fargo Letter*, *supra* note 50.

<sup>114</sup> Steelman Interview, *supra* note 90.

<sup>115</sup> *Id.*

feature is now standard on the ATM911 system, and SafeAlert Systems claimed it has greatly reduced the incidence of false alarms.<sup>116</sup>

The experience of Sharon Hill Borough, which mandated an alarm button system at outdoor ATMs, is that most activations of the alarm button have arisen from ATM customers who believe that pushing the button will call a customer service agent or a teller inside the adjoining bank, e.g., to request assistance in operating the ATM.<sup>117</sup> The Borough could not identify any incident where a dispatch resulting from the activation of the alarm button actually involved a crime.<sup>118</sup>

#### **D. Costs of Implementation**

SafeAlert Systems reported that the cost of implementing its ATM911 system on an ATM, including the costs of installation charged by the dealer, is approximately \$1,500.<sup>119</sup> SafeAlert Systems does not charge the users of its ATM911 system any licensing fees or royalties.<sup>120</sup> The company stated that ongoing maintenance costs were to be expected; it was unable to provide an estimate on these costs but expected them to be relatively small.<sup>121</sup>

---

<sup>116</sup> *Id.*

<sup>117</sup> Tinsley Interview, *supra* note 96.

<sup>118</sup> *Id.*

<sup>119</sup> Steelman Interview, *supra* note 90. SafeAlert Systems also offers an option (for an additional charge) that allows up to three ATMs (e.g., one drive-up and two walk-up ATMs) to operate from a single ATM911 system. *Id.*; *see also* <http://www.safealert.com/about.shtml> for descriptions of other options for the ATM911 system.

<sup>120</sup> Steelman Interview, *supra* note 90.

<sup>121</sup> *Id.* SafeAlert Systems emphasizes that ATM911 does not require the installation of an additional phone line. Rather, the system can operate on a fax line already connected to the ATM. When the alarm button is pushed, the system “will automatically seize use of the telephone line and call 911. All calls on the system are made directly to the 911

Bank of America identified as a cost of an alarm button system “additional FTE [full-time employees] required to support communications to [a] security command center to provide law enforcement with specific details regarding incidents specific [to] ATMs.”<sup>122</sup> It is not clear, however, whether Bank of America was basing its cost assessment on the system offered specifically by SafeAlert, which simply activates a call channel for operator listening, and would not likely require the deployment of additional bank employees.

## **V. Conclusion**

FTC staff’s investigation revealed that requisite data to evaluate the efficacy of ATM emergency-PIN and alarm button technologies are not available. The best available qualitative information – obtained from staff’s review of past government investigations into ATM emergency-PIN technologies and responses received from trade associations, banks, patent holders, and others regarding the relative costs and benefits of these devices – suggests that these technologies: (1) may not deter any type of ATM crime, and in some instances may actually increase the risk of danger to ATM customers; (2) might entail banks incurring non-trivial costs for their deployment; and (3) could result in at least some false activations that might lead to the inefficient allocation of police resources. The information obtained by staff does not allow the staff to obtain an estimate of the costs of implementing emergency-PIN or alarm button technologies, nor

---

Dispatcher. There is no need for a monthly monitoring charge!” See <http://www.safealert.com/ProductDescription.shtml>.

<sup>122</sup> See *Marc Lyons E-mail II*, *supra* note 57 (wherein Bank of America also notes that the installation of ATM alarm buttons would involve the “cost associated with purchase [and installation] of physical alarm devices at each of 18,000 [Bank of America] ATMs”).



does anecdotal evidence reviewed by FTC staff allow for any definitive conclusions about whether the reviewed emergency-PIN or alarm button systems reduce ATM crimes.