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

Table of Contents

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 security, and suppliers of the technologies – that staff believed to be most likely to have relevant data on ATM crimes and security technologies. None of these sources, however, provided data that would permit the analyses specified by the Act. Most fundamental, FTC staff learned that emergency-PIN technologies have never been deployed at any ATMs, and alarm buttons have been deployed only at very few ATMs. None of the information collected indicated that any similar technology is currently in use for a distressed customer to electronically alert local law enforcement. FTC staff found that data on ATM-related crimes and the costs of these emergency technologies – whether from government or private sources – are very limited and are inadequate for a rigorous analysis.

The information staff received and staff's review of the state-level legislative history relating to these issues, however, raise questions about whether the benefits of emergency-PIN or alarm button technologies would exceed the associated costs of implementation for most ATM-related crimes. The available information suggests that emergency-PIN and alarm button devices: (1) may not halt or deter crimes to any significant extent; (2) may in some instances increase the danger to customers who are targeted by offenders and also lead to some false alarms (although the exact magnitude of these potential effects cannot be determined); and (3) may impose substantial implementation costs, although no formally derived cost estimates of implementing these technologies are currently available. The anecdotal evidence that the staff relied upon, however, does not allow for any definitive conclusions regarding the efficacy of the reviewed emergency-PIN or alarm button systems to affect ATM crimes.

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")[1] 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] . . . ."[2]

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] . . ."[3]
- "a mechanism on the exterior of an [ATM] that, when pressed, would summon a local law enforcement [officer] to such [ATM]."[4]

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."[5] The Commission is to issue

[1] Credit CARD Act of 2009, Pub. L. 111-24, § 508.

[2] *Id.* at § 508(a).

[3] *Id.* at § 508(a)(1).

[4] *Id.* at § 508(a)(2).

[5] *Id.* at § 508(b)(1)-(4).

a report of the findings of the study no more than nine months after the date of the enactment of the Act. The report is also to include "such recommendations for legislative action as the Commission determines appropriate."[6]

FTC staff found that a few security systems allowing a distressed ATM customer to contact a local law enforcement agency electronically have been developed. However, no federal or state laws or regulations currently require the adoption of such measures, and FTC staff found no evidence that any of these proposed technologies have been deployed to any significant extent.

Staff obtained a variety of anecdotal data, but was unable to find data sufficient to conduct a rigorous study of the issues set forth in the Act. This report describes the staff's efforts to collect the data, discusses the anecdotal data received, and concludes, based on that anecdotal data, that the benefits of these ATM security technologies might not exceed the associated costs. At the same time, this anecdotal evidence does not allow for any definitive conclusions regarding the efficacy of emergency-PIN or alarm button systems to affect ATM crimes.

II. Nature of Available Data

A. Background

FTC staff investigated a broad range of potential information sources regarding ATM crime and security technologies that would allow staff to perform a credible study. As mandated by the Act, FTC staff consulted the United States Department of Justice ("DOJ") and the Secret Service; it also contacted the Federal Deposit Insurance

[6] *Id.* at § 508(c).

Corporation ("FDIC").[7] FTC staff searched ATM trade industry publications and the academic literature related to ATM crime. Staff researched state laws and reviewed the records of states' consideration of legislation, and contacted state and local law enforcement as well as municipalities that it identified as having mandated installation of alarm buttons (along with cameras and other safety measures).

FTC staff asked members of industry that might have relevant data whether they maintain information on the security technologies installed at ATMs, as well as the crimes committed at those locations. Staff contacted a manufacturer of ATMs and provider of ATM security solutions, a major provider of electronic payment software, and two trade associations whose members include ATM manufacturers, banks, payment card networks, and information processors, among others. Staff also obtained information from three holders of patented ATM security technologies. Finally, FTC staff directly contacted private financial institutions (referred to here for simplicity as "banks").

FTC staff determined that no public or commercial organization appears systematically to collect or to have collected the ATM-related data that would be necessary for the Commission to conduct a rigorous study. First, as discussed below, no ATMs employ or have employed an emergency-PIN system, and very few employ an alarm button system. Staff found no indication that any other technology with the capability of allowing a distressed ATM customer to contact electronically a local law enforcement agency exists. Thus, it was not possible to derive a formal (*i.e.*, statistical) estimate of the number or severity of crimes deterred as a result of an emergency-PIN or

[7] *Id.* at § 508(a).

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.[8]

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 *fraud* is much more common than crime committed directly against ATM customers who are in the process of attempting to withdraw cash.[9]

B. Data from the Department of Justice

The DOJ, through the Federal Bureau of Investigation ("FBI") Bank Crime Statistics ("BCS") program, compiles some data on ATM crimes. The data have deficiencies, however, that render them unsuitable for the study mandated by the Act. The FBI's BCS data classify a reported offense at an ATM as a robbery, burglary, or

[8] Fraud crimes include the insertion of a "skimmer" device into an ATM card reader in order to steal a customer's PIN number as well as attempts to remotely "hack" into the software systems running ATMs and/or their networks in order to electronically divert funds into another account. Fraud offenses are not those in which a victim is "under duress;" rather, such crimes come to the victims' attention only after they have already been committed. Thus, adoption of an emergency-PIN or alarm button system would be expected to do little in deterring the incidence of ATM fraud.

[9] Telephone Interview with Jonathan Velline, Senior Vice President, ATM and Store Strategy, Wells Fargo (September 25, 2009).

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.[10] 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.[11] 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.[12]

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

---

[10] E-mail from Bradley V. Bryant, Unit Chief, Violent Crimes Unit, U.S. Federal Bureau of Investigation to FTC staff (July 15, 2009).

[11] *Id.*

[12] The FBI's BCS crime statistics consist only of reported ATM offenses, and it is unknown to what extent the underlying reporting rates correlate with actual offense rates. Furthermore, these data only correspond to those ATMs that are owned by an FDIC insured institution (or the National Credit Union Administration in the case of a credit union). Some ATMs are not owned and operated by financial institutions, but there is no publicly available information regarding what proportion of the nation's ATMs are owned by entities other than banks. In any event, these facts suggest that the BCS data do not constitute a random sample of ATM crimes.

conducting the study. For example, the reports used by the Los Angeles Police Department ("LAPD") include an option to indicate whether a reported crime corresponded to an ATM robbery. However, the LAPD states: "The reports have a specific box for an ATM robbery, that was originally the focus, but this fact alone will not tell you if the transaction was forced or after the monies had been withdrawn . . . ."[13]

Whether the crime occurred before or after the money is removed from an ATM is critical in evaluating the types of ATM security devices specified in the Act.[14] A customer who is confronted by a criminal only *after* he or she has withdrawn money from an ATM will not be able to activate an emergency-PIN, and, if confronted after moving away from the ATM, may not be able to activate an alarm button device. The LAPD indicates that only a detailed study of individual police reports could determine the precise circumstances surrounding these reported robberies.[15] Joseph Zingher, a patent holder of one emergency-PIN technology (discussed below), attempted to obtain ATM location-specific crime data from police jurisdictions that he identified as tracking these data, but those agencies would not examine the individual police records.[16]

---

[13] E-mail from Alfred Pasos, LAPD, to FTC staff (December 1, 2009).

[14] As discussed further below, one type of emergency-PIN technology is "reverse-PIN." Bank of America notes that "[an]other problem with reverse PIN to consider is that it assumes the customer is approached *prior* to entering their PIN as opposed to after they have started their transaction. There has been no study to determine whether the ATM robberies are committed before or after the customer enters their PIN." E-mail from Marc Lyons, Bank of America, to FTC staff (October 2, 2009) (*Marc Lyons E-mail*). On the other hand, the perpetrator may have some incentive to demand funds before the transaction is completed so as to force the customer to withdraw the maximum amount of funds allowed by the ATM.

[15] Pasos e-mail, *supra* note 13.

[16] Telephone Interview with Joseph Zingher, President, Zi Cubed Inc. (December 3, 2009).

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.[17] However, these banks indicated that they did not have sufficient data for the study.

[17] 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 provide a relatively accurate assessment of the current state of ATM security technologies and the extent of their adoption given the scale of their ATM networks. Furthermore, as discussed below, patent holders Mr. Zingher and the seller of ATMOnGuard indicated that no U.S. banks are currently using (or have ever used) emergency-PIN technology, which would render any further attempts to obtain data from banking institutions moot. Zingher Interview, *supra* note 16; Telephone Interview with Danalyn Russikoff, ATMOnGuard (February 1, 2010).

E. Summary

Because of the lack of sufficient data, FTC staff could not conduct a credible study of the issues specified in the legislation. The following discussion of the anecdotal information obtained addresses, in turn, emergency-PIN technology and alarm buttons.

III. Emergency-PIN Technology

A. Description and Use

An emergency-PIN (personal identification number) works by allowing a distressed customer at an ATM to enter some variant of their regular bank card PIN in the keypad to electronically alert a law enforcement agency. One variant of this technology, known as "reverse-PIN," has been rumored to have been available at ATMs for some time despite never being implemented, falling into the realm of urban legend.[18] Under a reverse-PIN system, a distressed ATM customer with a bank card PIN of, for example, "1234" would simply enter this number backwards, or "4321," which in turn would automatically send an electronic relay message to a dispatch center or the police, alerting them of the customer's location.[19]

[18] *See, e.g.*, http://urbanlegends.about.com/library/bl_reverse_pin.htm (noting that the availability of a reverse-PIN system at ATMs is only a rumor).

[19] A commonly cited criticism of the reverse PIN concept is the fact that many bank customers have "palindromic" PINs, such as "2222" or "4334," which are the same when reversed. The palindromic PINs thus may not provide for an alert to the police or may result in an accidental alert to the police. Mr. Zingher's SafetyPIN system (discussed below) offers a solution to these PIN combinations; in the former case a "plus one" algorithm is adopted (the reverse PIN associated with "2222" would become "3333"), while the latter uses an "inside out" algorithm ("4334" would become "3443").

An ATM reverse-PIN system called "SafetyPIN" was invented by Joseph Zingher and patented in March 1998.[20] 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."[21] 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)."[22] For several years, Mr. Zingher attempted to sell SafetyPIN to banks in Illinois, Georgia, and Florida, but his attempts were unsuccessful.[23] Mr. Zingher offered to make the product available for free on a trial basis to banks in Kansas, but his offer was declined.[24] 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.

---

[20] 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/.

[21] 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).

[22] Letter from Joseph Zingher to FTC staff (November 30, 2009) (*Zingher Letter*).

[23] Forbes: Banking on ATM Safety, *supra* note 21.

[24] *Id.*

Another emergency-PIN system currently marketed to banks is "ATMOnGuard."[25] This device, which Mr. Zingher identified as a competing product,[26] 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.[27] The ATMOnGuard system has never been deployed at any ATMs in the U.S.[28]

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.[29]

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.[30] However, before enactment, the bill was amended to make the use of this technology discretionary.[31] The issue

---

[25] *See* http://atmongurard.com/; Computerized Password Verification System and Method for ATM Transactions, U.S. Patent No. 6,871,288 (filed February 21, 2003) (issued March 22, 2005).

[26] *Zingher Letter*, *supra* note 22.

[27] *See* http://www.atmonguard.com/system/index.htm.

[28] Russikoff Interview, *supra* note 17.

[29] Interview with Dean D. Stewart, Director, Self-Service Portfolio Management, Diebold, Inc. (March 1, 2010).

[30] *See* S.B. 562, 96th Gen. Assem., Reg. Sess. (Ill. 2003).

[31] *See* Illinois General Assembly, Public Act 93-0273 (eff. 1-1-04) ("A terminal operated in this State *may* be designed and programmed so that when a consumer enters his or her

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.[32] 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.[33] This bill was not enacted. In 2006, the Georgia State Assembly considered a measure that would have adopted reverse-PIN systems on ATMs.[34] 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).

[32] *See* S.B.1355, 96th 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 . . . ."

[33] S.B. 333, 2004 Leg., Reg. Sess. (Kan. 2004).

[34] *See* S.B. 379, 148th 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.[35] 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

[35] *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: STICKUPS AND STREET CULTURE (1997)).

> decreased from approximately one crime per one million ATM transactions to one crime per 3.5 million transactions.[36]

In addition, as discussed above, many kinds of crimes often described as ATM crimes would not be affected by use of the technology.[37]

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.[38] Indeed, with regard to SafetyPIN, some commenters have argued that it is

---

[36] 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. ATM robberies. Estimates are derived from periodic surveys of banks conducted by banking associations. According to those surveys, there was an estimated one ATM crime (including robbery) per 3.5 million transactions. Statewide surveys conducted in California indicated there was one ATM crime per 1.9 million transactions in 1986, one per 1.2 million in 1992, and one per 2.5 million in 1995. Thus, the California figures suggest that the rate of ATM crime declined by about 50 percent during that brief period, although we do not know how well the bank survey data reflect the actual incidence of ATM crime. Moreover, the surveys covered all ATM-related crimes, not just robbery, so the figures overstate robbery rates.
>
> The survey figures and findings are still cited as if they reflect current conditions, even though it is doubtful that they do. The best one can conclude is that the overall rate of ATM related crime is somewhere between one per 1 million and one per 3.5 million transactions, suggesting that such crime is relatively rare. But the figures, without further analysis and some comparative context, do not tell us much about the risks of ATM robbery. Local analysis of ATM robberies will be necessary to determine how significant the problem is in your jurisdiction.

[37] *See supra* Section II.A.

[38] As discussed below, the type of ATM-associated crime that Mr. Zingher and the seller of the ATMOnGuard system emphasize in their marketing efforts is "express

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.[39] 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.[40]

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.[41]

As such, the Office could only recommend further study into the efficacy of reverse-PIN technologies.[42]

---

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 potentially murders the victim. The concerns raised herein regarding the efficacy of ATM emergency-PIN devices would also seem to apply to express kidnappings.

[39] *See, e.g.*, *ATM Report*, *supra* note 36, § III:

> [H]uman behavior must be taken into account. Being surprised by the threat of bodily harm is extremely stressful. Severe stress such as this impairs the thought process. Under these conditions, it is difficult enough for many people to remember their correct PIN number. It may be asking too much of a consumer to try to remember a second emergency PIN. Criminals will undoubtedly be among the first to know of a reverse PIN system and how it works. Any delays or glitches incurred by a victim during an ATM crime could cause the criminal to physically harm the victim.

[40] *Marc Lyons E-mail*, *supra* note 14.

[41] *See ATM Report*, *supra* note 36, § I.

[42] Obviously, any assessment of the efficacy of the relevant ATM security technologies depends upon how both potential victims and criminals will alter their behavior in response to the technologies being made available. The staff is not aware of any studies that have carefully considered the behavioral or psychological processes of victims or offenders in the presence of such technologies.

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.[43]

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.[44] Thus, in a majority of instances, police response times to violent robberies would exceed that necessary for interrupting the crime or apprehending the offender.[45] Nonetheless, responses within 5 minutes were not infrequent. Also, the potential for such a response

[43] 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.

[44] 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.

[45] 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.[46] 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

[46] 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" (also referred to as "forced withdrawals").[47] These crimes involve an offender abducting a victim, taking him or her to an ATM (or approaching the victim while he or she is in the process of withdrawing money), and having the victim withdraw funds from their bank account (by either coercing the victim to enter his or her PIN or by revealing the PIN to the criminal). The criminal may then forcibly take the victim to other ATM locations in order to force the withdrawal of more funds from the victim's account. By definition, these crimes necessarily involve the offense taking place before or during the time the victim is using the ATM, and as such, potential temporal displacement effects may not apply. But again, whether distressed customers would be able or even willing to use emergency-PINs under express kidnapping scenarios is unclear, and the issue of police response times still applies in these cases.[48]

[47] *See Zingher Letter*, *supra* note 22; http://www.atmonguard.com/about/index.htm.

[48] Furthermore, some academic research suggests that it may be possible for criminals to partially "defeat" an emergency-PIN system even in the context of forced ATM withdraws – particularly those that rely on a "two-password scheme" such as SafetyPIN and ATMOnGuard – through so-called "forced randomization attacks." *See*, *e.g.*, Jeremy Clark & Urs Hengartner, Panic Passwords: Authenticating under Duress 6 (unpublished manuscript, *available at* http://www.cs.uwaterloo.ca/~j5clark/papers/panic.pdf). This possibility arises because criminals may become aware of the specific characteristics of the emergency-PIN mechanism put in place, and accordingly, adjust their behavior so as to decrease any possibility of being apprehended as the result of an ATM user activating an emergency-PIN.

C. Costs of Use

The use of an emergency-PIN system might increase physical danger to the victim due to the difficulties distressed customers may experience in using the system. The banks responding to staff's inquiries stated the belief that the real risk of customers fumbling to put in their PIN in reverse would result in a greater likelihood of personal harm befalling the customer if the perpetrator perceives the ATM customer as attempting to stall. In discussing the difficulties of using such a system, as described earlier, Bank of America stated: "There are also concerns that customers under stress may be unlikely to remember the reverse of their PIN, which may place them in greater danger should the perpetrator figure out what they are attempting to do and escalate the situation."[49] Wells Fargo concurred: "A customer under duress might have a difficult time remembering their alarm [emergency-] PIN . . . . A customer who is [contemplating] sounding an alarm [by activating their emergency-PIN] might try to unsafely delay a perpetrator in the hopes that police will quickly respond; this could worsen an already unsafe situation."[50]

---

[49] *Marc Lyons E-mail*, *supra* note 14.

[50] Letter from Jonathan Velline, Senior Vice President, ATM and Store Strategy, Wells Fargo to FTC staff (October 16, 2009) (*Wells Fargo Letter*). Wells Fargo goes on to note:

> Finally, none of these solutions *prevent* crime. If a crime is being committed, we believe the safest course of action is for a customer to comply with the demands of their attacker. The majority of Wells Fargo ATMs are equipped with surveillance cameras. Surveillance tapes can be examined to retrieve information and help law enforcement officials identify thieves. Wells Fargo customers are not liable for unauthorized ATM transactions when they use their Wells Fargo ATM debit card.

Id. (emphasis added). On the other hand, a critical limitation of security cameras is that offenders can simply disguise their appearance while committing offenses (*e.g.*, wearing a mask or hood), which makes identifying and subsequently apprehending the offender inherently more difficult.

Diebold Inc., a manufacturer of ATMs and provider of various ATM security solutions,[51] indicated that it has had numerous conversations with banking institutions regarding the implementation of an emergency- or reverse-PIN system.[52] 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.[53] Diebold concurs with this sentiment and does not believe that implementing an emergency-PIN system is prudent.[54]

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.[55]

---

[51] *See* http://www.diebold.com/solutions/atms/opteva/html/default.htm.

[52] Stewart Interview, *supra* note 29. *See also* http://www.diebold.com/atmsecurity/securityupdate.htm.

[53] Stewart Interview, *supra* note 29.

[54] *Id.*

[55] *ATM Report*, *supra* note 36, § III. In addition to the increased risk of physical harm, there is some possibility that ATM users might occasionally confuse their regular and emergency-PIN, thereby unintentionally setting off the duress signal and causing law enforcement to incur the costs associated with false alarms. For a discussion of the prevalence of false alarms in the context of duress or hostage codes used for home burglar alarm systems *see* http://www.faraonline.org/DuressResolution.pdf ("Alarm system users can easily get their Duress Code confused with their regular code. When the Duress Code is entered, the user believes he has turned the system off, not aware that armed law enforcement personnel may be responding to the signal in an escalated emergency mode. This creates an undesirable, dangerous situation for both the alarm user and the law enforcement personnel.")

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 technology has not been adopted for any ATM. Respondent banks, an ATM security firm, and a major provider of electronic payments software all reported that they have not developed any formal cost estimates of deploying and maintaining the technology.[56] One cost estimate offered by a potential supplier of the available technology is not based on any formal cost study. Further, potential purchasers of the technology, the potential supplier, and third parties define the cost components differently. The discussion below sets out the information and analysis of costs that FTC staff was able to identify.

1. Bank Cost Estimates

Bank of America provided FTC staff with a descriptive listing of the types of costs it believes would be incurred in implementing a reverse-PIN technology.[57] Bank of America maintains that software upgrades likely would be needed for individual ATMs

[56] For instance, Wells Fargo stated: "We have not estimated these costs, since we don't think the solutions are feasible." *Wells Fargo Letter*, *supra* note 50. Similarly, Citibank responded: "This [*i.e.*, a cost estimate for implementing emergency PIN or alarm button technologies] has not been studied and the information on cost is not available at this time." E-mail from Glen Mellone, Vice President, Citibank Security and Investigative Services to FTC staff (November 9, 2009).

[57] *See* E-mail from Marc Lyons, Bank of America, to FTC staff (October 9, 2009) (*Marc Lyons E-mail II*). Bank of America was unable to provide to the staff any dollar estimates of the various cost elements they identified pertaining to an emergency-PIN technology.

as well as for the central systems that run the ATM networks.[58] 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.[59]

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."[60] However, the respondent banks were unable to provide information on the extent to which the system would require integration greater than the currently existing systems, or any cost estimates to achieve such greater integration.

---

[58] *Id.*

[59] *Id.* Bank of America notes the costs of royalty payments as "unknown." *Id.*

[60] *Wells Fargo Letter*, *supra* note 50; *see also Marc Lyons E-mail*, *supra* note 14 ("Operational challenges also exist if another bank's cardholder is using our ATM . . . . The ATM networks currently do not possess the technology to verify the cardholder's reverse PIN and pass that message over the network to the ATM owner/operator, along with the additional message to call the police.").

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.[61] 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.[62] Mr. Zingher's estimate implies that the total cost of upgrading the approximately 400,000 ATMs deployed across the U.S.[63] 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

---

[61] *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.

[62] Zingher Interview, *supra* note 16; *Zingher Letter*, *supra* note 22.

[63] 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.

kidnapping scenario. Furthermore, having access to this information may prevent law enforcement from potentially mistaking the victim for the offender.[64] As such, SafetyPIN would require interconnection with state government drivers' license computers and databases both within and across states, and possibly even internationally. It is not clear whether Mr. Zingher's cost estimate reflects the initial and recurring expenses associated with establishing these particular interconnection routes.

Mr. Zingher's estimate assumes that there is already a form of emergency-PIN system in place on the ATMs.[65] Mr. Zingher provided no details about the proportion of the estimated 400,000 ATMs in the U.S. that possess this type of alarm system, and FTC staff do not possess sufficient information to assess this claim.

Mr. Zingher's analysis presumes that the alarm sent by the emergency-PIN system would be received by a burglar alarm company, rather than directly by law enforcement. The estimate does not include any new expenditure by law enforcement to receive electronic messages directly.

---

[64] *See Zingher Patent*, *supra* note 20; *Zingher Letter*, *supra* note 22; *ATM Report*, *supra* note 36 § III ("In addition to the location of the ATM, police could find out who the customer was with information taken from the customer's bank account records. Police could also access a description of the customer from the Secretary of State's Drivers' Services Division. By the time police reach the ATM they would know who the customer is, what s/he looks like, and where s/he lives.").

[65] Mr. Zingher stated:

> One of the reasons that the cost of installing the completed system is so low is that [there is] already an emergency PIN system in place on the ATM. It is for the benefit of the employee who loads the cash into the ATM. The message routing is already available at the burglar alarm company that monitors the ATM. The burglar alarm company just gets the alert from my system instead of the keypad the worker uses.

E-mail from Joseph Zingher to FTC staff (December 3, 2009).

The estimate apparently does not include licensing and royalty costs. Mr. Zingher stated: "The licensing costs, the royalties paid to the patent owners are really imponderable. Whatever the market will bear is the only reasonable thing to say."[66] Mr. Zingher's estimate also apparently does not include maintenance costs for the software or physical equipment, or any added staff costs.

The seller of the ATMOnGuard system was unable to provide the staff with a cost estimate of deploying their technology at ATMs.[67] The seller is currently attempting to arrange a series of trials for the deployment of their system with various banks – which could inform a cost estimate – but so far no such trial has been initiated.[68]

3. Third-Party Cost Estimates

Diebold, Inc., which manufactures ATMs and ATM security systems, stated that the implementation of an emergency-PIN system is technically feasible and would not likely require any changes (physically or otherwise) to the individual ATMs themselves.[69] The company indicated that any software modifications needed to implement an emergency-PIN system would occur at the "host end," specifically, at the software that runs the host security module ("HSM"), which is a hardware component.[70] The function of the HSM is to run the PIN verification system, which includes decrypting

[66] *Zingher Letter*, *supra* note 22.

[67] Russikoff Interview, *supra* note 17.

[68] *Id.*

[69] Stewart Interview, *supra* note 29.

[70] *Id.*

PINs sent over the ATM network and making the requisite PIN "comparisons" (i.e., verifying that the PIN entered by the customer is the correct one).[71]

Diebold stated that modifying the HSM software to implement the reverse-PIN version of an emergency-PIN system "would be complex" and that the modifications might affect transaction processing speeds (but not to an extent that would noticeably affect the speed at which a withdrawal was made as compared to a regular PIN).[72] According to the company, the HSM software would have to be modified in order to handle a larger number of PINs requiring processing under a reverse-PIN system, while also conducting more PIN verifications. Diebold indicated that the modifications would likely be in the thousands of dollars per machine but was unable to provide a precise cost estimate to modify the HSM software to implement a reverse-PIN system.[73] Finally, Diebold indicated that some additional expenses probably would have to be incurred by banks in order to process duress messages sent out by a customer activating a reverse-PIN,[74] such as additional employees to handle the communications between the alarm dispatch center and any other relevant entities. Diebold stated that it generally agrees with financial institutions regarding the costs that banks would have to incur in order to modify the ATM backbone network (as opposed to costs of reconfiguring individual ATMs themselves) in order to implement a reverse-PIN system.[75]

---

[71] *Id.*

[72] *Id.*

[73] *Id.*

[74] *Id.*

[75] *Id.*

ACI Worldwide, a major provider of electronic payments software, including the software that runs the HSM,[76] 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.[77] The company never completed the cost study because the requirement was never enacted.[78] 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.[79]

The State of Illinois ATM Report noted four significant "computer interface barriers" to an effective reverse-PIN system:[80]

- First, are the limitations inherent in the use of PIN numbers. The system would double the amount of PINs used per person.[81]

- 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

[76] Interview with Richard A. Duval, Senior Strategic Alliance Manager, ACI Worldwide (March 3, 2010).

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

[78] Duval Interview, *supra* note 76.

[79] *Id.*

[80] *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.").

[81] *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 of State's office for driver license information.[82]

- Third, most law enforcement agencies do not have the computer capacity to provide the necessary real time communication with an ATM. Many police 911 units respond only to voice communication, although some are now taking calls via the internet. In addition, there is no assurance of immediate response by police agencies. This may result from the huge number of calls handled in urban areas to the geographic separation that occurs in rural locations.[83]

- Fourth, the cost to reconfigure the ATM system, including shared ATM networks, can be quite high . . . . The physical reconfigurations needed to make changes to machines have been estimated at $1,500.00 to the thousands of dollars each. The minimum impact is estimated to be at least $7,500,000.00 [for ATMs regulated by the Illinois Office of Banks and Real Estate]. This does not include the software programming costs. This estimate does not include the additional costs associated with thousands of ATMs in Illinois that are not regulated by the Office of Banks and Real Estate. To be fully functional, the [emergency-PIN] system would have to have communication capabilities with financial institutions worldwide in order obtain customer account information. The system would likewise have to communicate with driver license agencies or similar authorities worldwide to obtain descriptive information about the victim.[84]

These barriers led the Illinois Office of Banks and Real Estate to conclude that "significant barriers exist in the application of reverse-PIN systems at this time."[85]

Staff also contacted two ATM-industry trade associations, the ATM Industry Association and the Electronic Funds Transfer Association,[86] to determine if they had any

---

[82] *Id.* Communication with the office for driver's license information is required in order to provide the responding police officer(s) with a physical description of the distressed ATM customer, including a driver's license photo.

[83] *Id.*

[84] *Id.* The report does not provide any further information regarding the source of the cost estimates cited therein.

[85] *Id.* Mr. Zingher refutes the Illinois conclusion that implementing a reverse PIN solution would require any physical reconfiguration of individual ATM machines. *Zingher Letter*, *supra* note 22.

[86] *See* http://www.atmia.com/ and http://www.efta.org/, respectively.

relevant data concerning the costs of deploying an emergency-PIN system. Neither of these entities was able to provide such information.[87]

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-PIN systems will have little or no effect, or that they will even increase injury (although to what extent is not certain). The anecdotal evidence that the staff relied upon does not allow for any definitive conclusions regarding the efficacy of the reviewed emergency-PIN systems to affect ATM crimes.

IV. Alarm Button Technology

A. Description and Use

FTC staff identified a single manufacturer of an ATM user alarm button technology, SafeAlert Systems, which sells its patented "ATM911 Emergency Communications System" (hereafter "ATM911"). According to the company:

> [ATM911] works similar to a programmable speaker telephone. When someone using an ATM feels that they have an emergency situation, they will push the 911 button. Within moments, the local 911 dispatcher answers the call and can be heard at the ATM unit. The 911 dispatcher will not only be able to hear the

[87] E-mail from Michael Lee, Chief Executive Officer, ATM Industry Association to FTC staff (March 3, 2010); Interview with Dennis Ambach, Chairman, Legislative and Regulatory Council, Electronic Funds Transfer Association (March 4, 2010).

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

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

SafeAlert Systems has sold alarm button systems for about 2,000 individual ATMs over the past 18 years.[91] 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.[92] 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.[93]

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.[94]

---

[88] http://www.safealert.com/How.shtml.

[89] http://www.safealert.com/ProductDescription.shtml.

[90] Interview with Larry Steelman, Vice President, SafeAlert Systems (February 25, 2009).

[91] *Id.*

[92] *See supra* note 63.

[93] Steelman Interview, *supra* note 90.

[94] *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.[95] 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.[96] Only one of the ATMs in the Sharon Hill Borough is located outdoors, and it has an alarm button.[97]

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.[98] 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.

---

[95] *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).

[96] Interview with Chief Robert Tinsley, Borough of Sharon Hill Police Department (March 2, 2010).

[97] *Id.*

[98] Steelman Interview, *supra* note 90; *see also* Final Report, *supra* note 61, at 6.

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 Police Department to install emergency "911" alarm buttons on several Wells Fargo ATMs in Oakland. These alarms were installed at the request of the Police Department based on concerns of crime occurring in the vicinity of the ATM. The experiment lasted less than six months and was removed at the request of the Police Department based on a deluge of false alarms. Out of the 500 alarms we had during the pilot program not one was legitimate or found to have merit.[99]

The Sharon Hill Borough ordinance was prompted by a murder at the only outdoor ATM location; however, the crime in question did not actually involve an ATM-related offense but rather a confrontation between two men that just happened to occur at the location.[100] The Borough could not identify any incident where a dispatch resulting from the activation of the alarm button actually involved a crime.[101]

While SafeAlert Systems recommends against pressing an alarm button during an incident, it claims that the mere presence of the button may serve as a deterrent to prevent ATM crimes from being committed in the first place at those machines where the system

---

[99] *Wells Fargo Letter*, *supra* note 50.

[100] Tinsley Interview, *supra* note 96.

[101] *Id.*

is installed.[102] However, it was not aware of any formal studies that have evaluated the effect of the technology on crime.[103]

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]."[104] 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."[105]

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

---

[102] http://www.safealert.com/How.shtml.

[103] 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*.

[104] Letter from Kenneth E. Patton, Mayor, City of Brooklyn to New Jersey Assemblyman Neil Cohen (August 2004).

[105] 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.[106]

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.[107] 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.[108] In addition, widespread deployment of alarm button systems at all ATMs over a broad geographic area could result in "temporal displacement,"[109] 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.[110] Because police reports and records may not detail the fact that a robbery

[106] The City of Strongsville ordinance also mandated specific lighting levels around ATMs, *see id.*, which further obfuscates any potential determination of the deterrent effect that might pertain specifically to the adoption of the ATM911 system.

[107] Steelman Interview, *supra* note 90.

[108] A 1993 study conducted by the Chicago Police Department concluded that overall crime rates would likely not be affected by ATM security devices, such as panic buttons, because they "would likely just result in the movement of crime to different locations where victims are more susceptible." *See ATM Report*, *supra* note 36, § IV.

[109] *See supra* Section III.B.4.

[110] It is also unknown to what extent any observed decrease in ATM crimes following the introduction of alarm buttons might simply reflect changes in the behaviors of law enforcement or ATM customers. Police may respond to an ATM crime by increasing their monitoring of ATM locations or by patrolling the areas surrounding ATMs more frequently at the same time alarm buttons are installed. Any reduction in ATM crimes may stem from the increased police presence rather than from the installation of alarm buttons *per se*, but it is difficult to separate their respective effects given the available

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.[111] 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.[112]

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 the customer; this risk may be higher for alarm buttons as the buttons are highly visible and it is unlikely that customers can press them without offenders knowing. As discussed earlier, law enforcement generally

---

data. Similarly, in the wake of an ATM crime ATM users may either avoid using those ATMs at which an offense took place or change the manner in which they use ATMs (e.g., only withdrawing money during the day when a large number of persons are present, not using ATMs as frequently, only withdrawing cash at supermarkets or at ATMs located inside buildings). If such changes in ATM user behavior are correlated with the deployment of alarm buttons, there is a risk of incorrectly attributing any observed reduction in ATM crime as stemming from the deployment of the alarm buttons themselves.

[111] *See supra* Section III.B.2.

[112] *See supra* Section III.B.1.

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.[113] 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.[114] The company claimed that Wells Fargo would not share specific information regarding the nature of the false alarms after the pilot program was terminated.[115] 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

[113] *Wells Fargo Letter*, *supra* note 50.

[114] Steelman Interview, *supra* note 90.

[115] *Id.*

feature is now standard on the ATM911 system, and SafeAlert Systems claimed it has greatly reduced the incidence of false alarms.[116]

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.[117] The Borough could not identify any incident where a dispatch resulting from the activation of the alarm button actually involved a crime.[118]

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.[119] SafeAlert Systems does not charge the users of its ATM911 system any licensing fees or royalties.[120] 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.[121]

---

[116] *Id.*

[117] Tinsley Interview, *supra* note 96.

[118] *Id.*

[119] 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.

[120] Steelman Interview, *supra* note 90.

[121] *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."[122] 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.

[122] *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.