

Turning Phishing into Cash: Criminal Convenience at the ATM?



Jerry Silva

Service Director

Aug 2005

Reference # V44:21NRCK

TowerGroup Take-Aways

- Although phishing can be an effective way to gather information used to commit online fraud, its use in creating counterfeit plastic involves an arduous path that limits its success.
- The automated teller machine (ATM) and point-of-sale (POS) devices, while suffering from their own brands of fraud, seem to be well protected from counterfeiting through phishing by the hurdles imposed by authentication codes on the magnetic stripe.
- Phishing has become a serious threat to those using the Internet to conduct banking transactions, causing mild inconvenience at best and life-changing misery when it leads to identity theft or account takeover.
- Large US banks confirm that an extremely small amount of phishing ever leads to loss from ATM or POS fraud, confirming that it is difficult to produce counterfeit debit cards - although smaller institutions have seen a rise in this kind of activity.
- Seen in perspective, fraud committed as a result of phishing still takes a back seat to other types of fraud, including credit card and check fraud.

Two Charles River Place
63 Kendrick Street
Needham, MA 02494
United States

T +1.781.292.5200
F +1.781.449.6982
towergroup.com

Report Coverage

Widespread accounts of the epidemic of phishing attacks on banking customers have the industry concerned about other possible channels where the information gained through phishing may be used to commit additional fraud. This TowerGroup Research Note looks at the possibility that phishing may be contributing to debit-based fraud at the automated teller machine (ATM) and at the point of sale (POS). In an already confusing landscape, where public perception matters almost as much as fact and where institutions hesitate to offer any details about sources and actual losses to fraud, this Note reports on the scale of phishing as the origin of fraud and explains how that crime affects the ultimate source of quick cash, the ATM.

Background

Phishing, the illegal act of soliciting personal and account information from bank customers through a bogus e-mail or Web site, is a plague affecting all financial institutions globally. Although the crime has been around since the late 1990s and blossomed in 2003, phishing has been linked more recently to the widely publicized reports of account takeover and identity theft, in which the perpetrator gathers enough information from the victim to impersonate that person and empty accounts or create new credit relationships. The impostor's opening of new accounts, for which the true customer is mistakenly held liable, requires perhaps the most effort for the customer to recover credit worthiness. The customer must first prove that he or she is not at fault, and that customer's credit history must be cleansed to repair the damage wrought by the criminal. For more information on phishing, see TowerGroup Research Note V41:10PCN, *A Phish Tale? Moving from Hype to Reality*.



Phishing for ATMs?

With increased reports of automated teller machine (ATM) and point of sale (POS) debit fraud occurring today, the banking industry is concerned about a possible link between phishing and the use of stolen information at these channels to convert that information more quickly into cash. In theory, the information gathered during a phishing attack could be used to create plastic cards, which could then be used at the ATM and POS to withdraw cash or purchase goods, respectively.

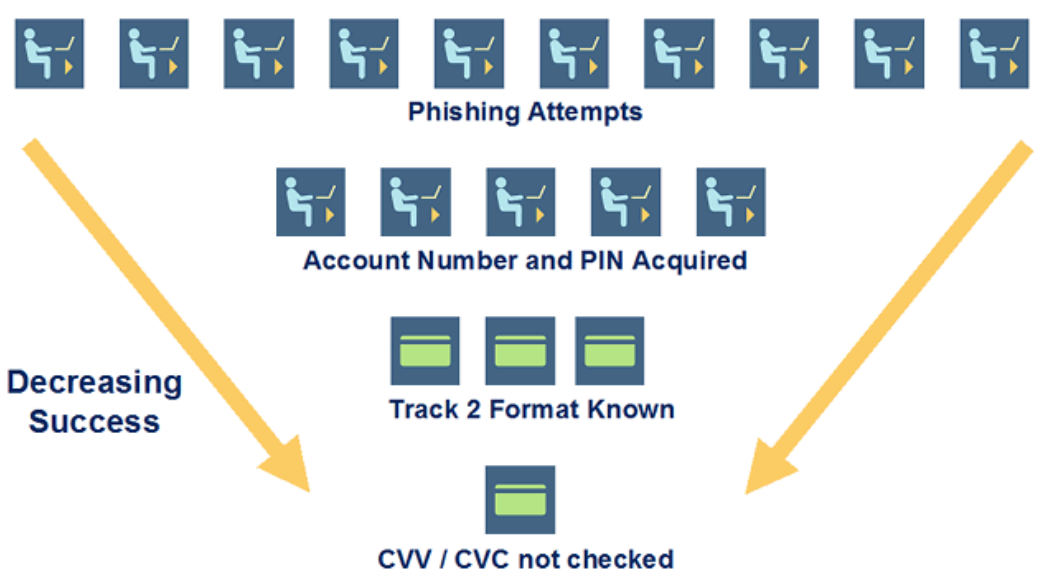
Getting naive customers to enter their account (or card) number and PIN is not the hard part, but to create counterfeit plastic, the criminal must know the data format of the magnetic stripe on the back of the card (usually referred to as "track information"). Learning the format is difficult but not impossible because the format is a widely known standard in the industry. Then the criminal must somehow recreate the card verification value (CVV) or card validation code (CVC), which are authentication codes created by Visa and MasterCard, respectively, to ensure that the physical card is present during a transaction. This step is impossible, for all intents and purposes, because the customer doesn't know what that encoded value is on the stripe. The CVV2 or CVC2 code, usually printed on the front or back of the card, is the only part the customer actually sees. However, this value merely represents the "answer" to an algorithm that uses the encoded CVV or CVC on the stripe, which is known only to the issuer. Phishing for the CVV2 or CVC2 value does not provide enough information to replicate the CVV or CVC on the stripe itself.

But there is one last hope for the villain: Although most ATMs and POS devices read and transmit the codes to the issuer for authorization, it is up to the issuer to check for these codes when authorizing the transaction. The CVV and CVC codes were created in part to ensure that the card is present during mail order and telephone order transactions (MOTOs). Since the ATM requires the card to be present during a transaction, the CVV and CVC codes were seldom checked during the interaction in the past. In fact, not all institutions check for these codes today; the verification of CVV and CVC is a process that has been implemented at most larger institutions only in the last 3 to 5 years. While TowerGroup estimates that over 90% of the top 100 banks in the United States check for CVV and CVC today, a high percentage of smaller banks probably do not.

Based on this chain of ever-increasing difficulties (creating a phishing attack, getting responses from customers, creating plastic with valid track formats, and targeting banks that do not check CVV or CVC) TowerGroup believes that the amount of ATM and POS debit fraud originating from phishing today is only about 3.5% of all fraud at those channels. Exhibit 1 depicts all of the components of a phishing scheme at the ATM and POS.



Possibility of Phishing Fraud via an Automated Teller Machine and at Point of Sale (2005)



CVV = Card verification value.
CVC = Card validation code.

Exhibit # 44-21NRCK-E1
Source: TowerGroup

Exhibit 1
Possibility of Phishing Fraud via an Automated Teller Machine and at Point of Sale (2005)
Source: TowerGroup

But ATM Fraud Does Happen

Based on recent discussions with the largest card-issuing US banks, TowerGroup estimates that on average, about one in 15,600 ATM and POS debit transactions today is fraudulent. Given an annual volume in ATM and PIN-based POS transactions of just over 17 billion in the United States last year, that means that about 1.1 million fraudulent debit transactions occurred in 2004. While most banks will not publicly release data on monetary losses from fraud, TowerGroup believes that withdrawal and debit purchase limits on retail accounts restricted total ATM and POS fraud losses to not more than \$990 million in the United States in 2004.

So if the fraud isn't primarily coming from phishing, where is it coming from? Based on information from large card issuers, it seems the "tried and true" sources of debit card fraud are still at work today, along with one new twist. Most debit card fraud occurs when a card is stolen or "borrowed" by a family member or friend with knowledge of the PIN. It stands to reason that this kind of fraud is the easiest to commit and thus represents the highest incidence of total debit card fraud. Stealing a card from a stranger's mailbox would still require some way to get the associated PIN, so while possible, this alternative is atypical.

A second and relatively recent source of card fraud comes from "skimming," the act of illicitly recording the information on the magnetic stripe while the customer is performing a transaction at an ATM or POS device. In card skimming, a phony card reader is attached to a real ATM or POS device to surreptitiously capture card information from the magnetic stripe, from which counterfeit cards can be made from blank stock. There is usually a hidden camera or other device or a person



who captures the PIN as the customer enters it. The latest form of skimming comes from the relatively "new" convenience store ATM market, in which sometimes unscrupulous independent deployers install ATMs for the sole purpose of card skimming. Customers whose cards are skimmed at such a machine have no clear way to delegate responsibility or recover loss because the machine is not run by a bank. Between stolen cards and skimming, US institutions lose almost \$1 billion every year to ATM and POS scams.

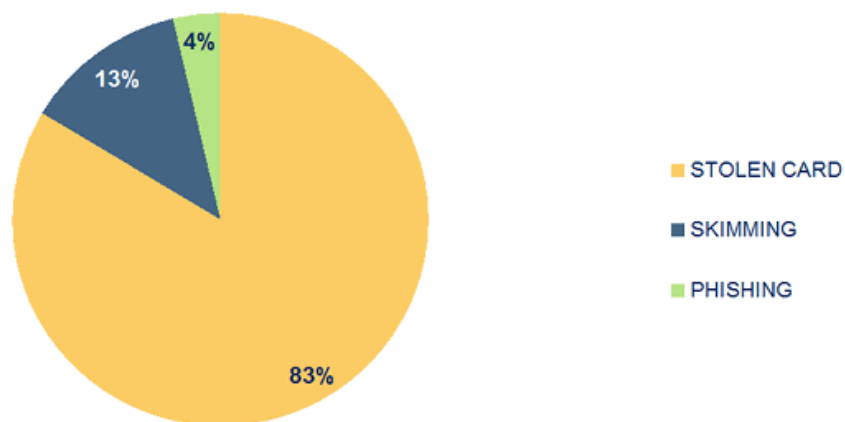
It may frighten many people to learn that this process is fairly straightforward and is not often detected by the consumer. The incidence of card skimming has increased at an alarming rate over the last five years, and ATM manufacturers are quickly developing anti-skimming tactics to help prevent skimming schemes. Nonetheless, the US Secret Service estimates that fraud losses from skimming are running at a rate of about \$350,000 a day in the United States. Skimming is a powerful fraud source because the bogus card reader captures the entire magnetic stripe, including the CVV or CVC, thus giving the criminal the ability to clone the card perfectly.

Still, phishing does seem to account for some fraud loss at the ATM and POS channels. Banks report that about 3.5% of fraudulent pin-based debit transactions are from counterfeit cards that were probably created through phishing. The low rate limited phishing-related ATM and POS losses to a maximum of \$35.5 million in 2004. Criminals will target fast conversion to cash at the ATM and high-value items to purchase at POS, counting on a \$500 to \$1,000 upper limit on debit cards. Considering the typical ATM withdrawal limit of about \$500 per day, the findings indicate an ATM fraud event occurs in just under two days, consisting of almost two withdrawals before the customer discovers the theft and calls to cancel the card. This is certainly a reasonable possibility and even more reasonable for cards that have higher limits.

Exhibit 2 shows the breakdown of US ATM and POS debit fraud by source in 2004.



US ATM and PIN-Based POS Debit Fraud by Source (2004)



Total US ATM and PIN-Based POS Debit Fraud Loss in 2004: \$990 Million

Exhibit #: 44-21NRCK-E2
Source: TowerGroup

Exhibit 2
US ATM and PIN-Based POS Debit Fraud by Source (2004)
Source: TowerGroup

Phishing in Perspective

Phishing has received widespread attention and has the potential for serious losses from account takeover and theft of funds for any given event. For victims, cleaning up their credit records after the theft of their identity through any means, including phishing, is onerous and unpleasant and can take many years.

But despite the publicity about phishing, TowerGroup interviews with the largest card-issuing banks in the United States and overseas revealed that phishing is most often found to be the source of theft through online access to consumer accounts, not through ATM or POS transactions. Even so, TowerGroup estimates that theft through phishing actually accounted for a relatively small global loss of about \$137 million in 2004. The phishing loss of \$81 million in the United States in 2004 represents, for example, less than 5% of the US credit card fraud loss of \$1.8 billion in 2004. (That is not to say that fraud from phishing accounted for 5% of credit card fraud.) When set against check fraud, which has been around since the beginning of banking, losses from phishing compare at a more respectable 13% of the \$677 million in check fraud based on the American Bankers Association reports. Although phishing itself does not automatically lead to fraud (and thus can't be directly compared with these fraud types), this analysis shows the relatively small contribution that phishing has made to banking fraud.

Exhibit 3 shows the relative size of losses from fraud for different payment types in the United States. Again, the phishing amount is shown only to provide a sense of scale as a source of fraud and not as a separate fraud type. See TowerGroup Research Note V41:08CPI, *Retail Financial*



Fraud: A Seismic Shift, for a more comprehensive treatment of the trends in fraud.

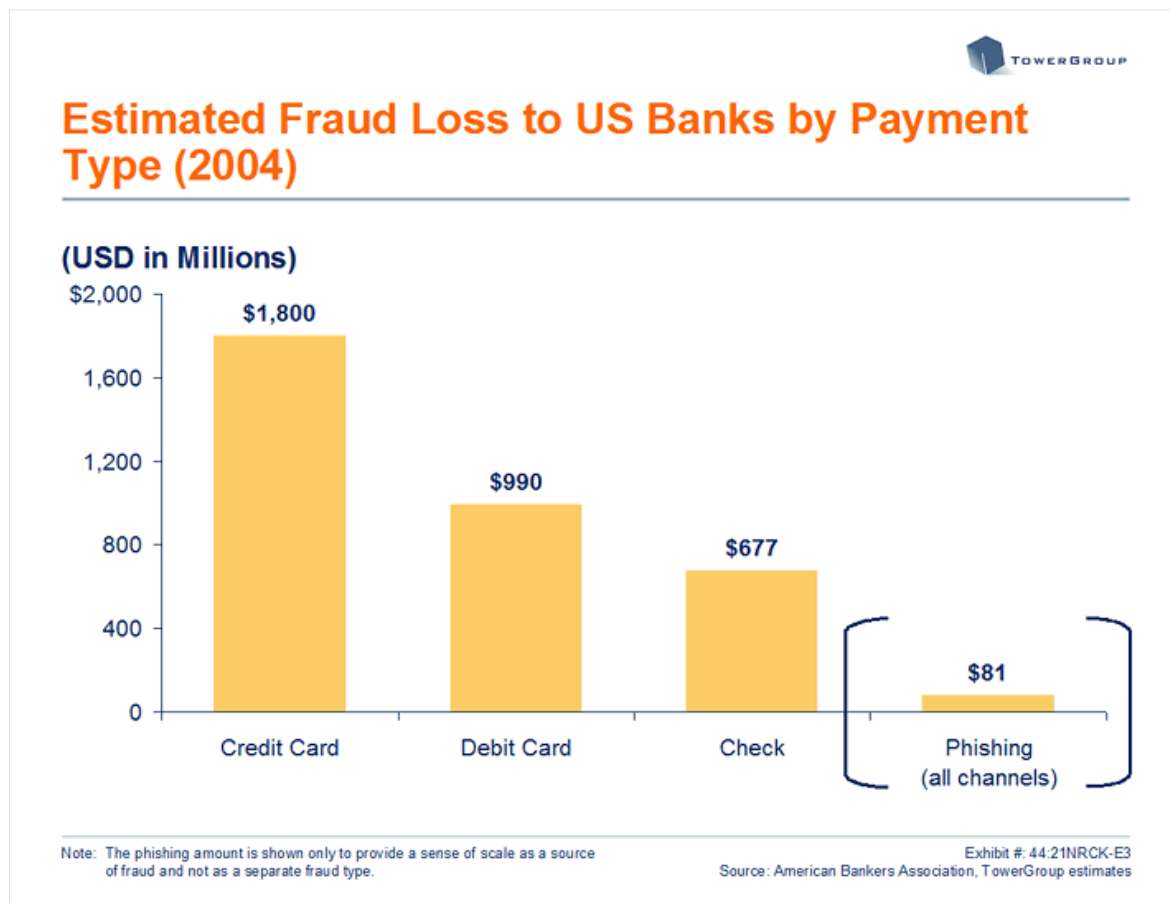


Exhibit 3
Estimated Fraud Loss to US Banks by Payment Type (2004)
Source: American Bankers Association, TowerGroup estimates

Summary

Phishing is a dangerous criminal act that can and does wreak havoc with its victims. The Internet has opened up a doorway through which not only phishing but key-logging and malware can record consumers' activities in the "privacy" of their own homes and turn against them to steal from them and impersonate them. On the bright side, in a reflection of the speed of Internet-based events, solutions to prevent phishing and respond to it have already been deployed by many institutions, barely 2 years since the first significant wave of this virtual crime. (See TowerGroup Research Note V41:11PCN, *No Phishing Zone: Vendor and Industry Initiatives to Curb E-Mail Fraud*.) The fact that losses through phishing are relatively small should offer some relief to institutions that are already battling fraud along many fronts. However, it should not lull those banks into a false state of relaxation. Phishing may not lead to the same scale of loss overall as credit card and check fraud do, but any victim of identity theft through phishing will attest to the enormous amount of damage it causes.

The ATM and POS channels are also seeing their share of fraudulent behavior, and card skimming is the most recent way to collect card information and use it to gain access to funds, either through withdrawal of cash or through fraudulent purchases. But it seems that the barriers between the ATM and POS devices and phishing are high enough to prevent most cross-contamination. The difficulties in creating counterfeit cards from plastic blanks and stolen customer information ensure that few attempts will be made. The increasing number of card issuers that check the secret authentication codes on the magnetic stripe further prevents any such cards from being used



successfully at the ATM or POS terminal. The largest card-issuing banks in the United States confirm that phishing is rarely seen as the source of debit card fraud, and although the banks won't divulge dollar losses from any specific kind of fraud, they do corroborate the relative scale of fraud loss estimated by TowerGroup. So although phishing may be the consumer threat du jour, there seems to be no evidence that the "phisher" is using the ill-gotten information to quickly turn the crime into cash.