ALM LAW JOURNAL NEWSLETTERS

THE PRIVACY & DATA PROTECTION LEGAL REPORTER™

Volume 1, Number 11 • December 2006

Online Banking's Battle Against Phishing

By Mark E. Plotkin and Michael Epshteyn

Online banking, which has seen explosive growth in recent years, has made it faster, cheaper, and more convenient than ever before for consumers to manage their financial affairs. It also holds the promise of significant cost savings for the financial services industry, as rising numbers of customers are expected to shift from over-the-counter services to online transactions.

Yet the adoption of Internet banking may be impeded if consumers lose trust in the security of online financial transactions. And while the reputation of online commerce has been affected by various high-profile data security breaches, such as the 2005 ChoicePoint debacle, consumer confidence in online banking is also threatened by "phishing," the insidious form of identity theft that uses fraudulent e-mails to lure victims to sham Web sites, where they are tricked into divulging ac-count numbers, passwords, and other sensitive information. Al-though there has been a sharp rise in the volume of phishing scams, and the techniques employed by "phishers" have grown more so-phisticated, banks and other entities have also become increasingly adept at detecting and combating phishing attacks. As this article discusses, there are a variety of steps that financial institutions can take to mitigate the risks posed by phishing and, at the same time, bolster their customers' online confidence.

Overview of Phishing

In a typical phishing attack, a consumer will receive an e-mail that purports to be from a financial institution, such as a bank, that the recipient knows and trusts. The e-mail — which bears the entity's trademark and logos, and a return address that appears to come from the company — will urgently request that the user update or verify his or her account information by clicking on an enclosed hyperlink. Ironically, recipients are often told that the e-mail has been prompted by fraudulent account activity and, in many cases, are threatened with some undesirable consequence, such as the suspension of their account, if they do not immediately comply. According to the Anti-Phishing Working Group ("APWG"), an industry association of corporations and law enforcement organizations dedicated to combating phishing, approximately 5% of those targeted in phishing attacks respond. When the recipient of a phishing e-mail takes the bait by clicking on an enclosed link, he or she is taken to a sham Web site designed to emulate the Web site of the legitimate business mentioned in the e-mail. There, the victim is asked to enter personal information, such as a login name, password, address, and social security number. Once this information has been submitted, the victim is typically redirected to the real homepage of the impersonated company, thereby giving an air of legitimacy to the fraudulent transaction. Indeed, given the veneer of authenticity of the entire process, phishing victims often do not immediately realize that their personal information has been stolen, and may not recognize the link between a phishing attack and subsequent financial fraud.

Once phishers have captured their targets' personal information, they can use it in a variety of ways. Some phishers use the stolen data to make online purchases or withdraw money from their victims' existing accounts. Others commit identity theft with the stolen information, establishing new accounts in the consumer's name. This type of fraud can be particularly devastating because it may remain undiscovered until the victim applies for a home or car loan, only to find that his or her credit has been destroyed. Phishers may also sell their victims' information to other cybercriminals, or trade it for software and computer equipment.

Phishing attacks have become increasingly sophisticated. Early phishers simply sent out mass e-mails, hoping that some of the recipients were customers of the impersonated entity. Today, many phishers engage in the more targeted practice of "spear-phishing," which involves sending messages to individuals known to have existing relationships with the mimicked institutions. While early phishing e-mails often were crude and marked by poor spelling, grammar, and punctuation, those sent today tend to be grammatically correct and, in many cases, are virtually indistinguishable from messages from the impersonated companies.

Likewise, in the past, the enclosed hyperlinks directed individuals to Internet addresses, or URLs, that bore no relation to the name of the purported sender; today, phishers have techniques for masking the URLs of their fraudulent sites and making the real company's Web site address

Mark E. Plotkin is a partner and **Michael Epshteyn** is an associate, practicing in the Financial Institutions practice group of Covington & Burling LLP's Washington, DC, office.

continued on page 2

Phishing

continued from page 1

appear at the top of a user's browser. Another tactic now favored by phishers is to direct consumers to a Web site that will surreptitiously install "malcode," or malicious software, onto their computers; once downloaded, these programs may hijack the victim's Web browser, record his or her keystrokes (allowing the phisher to capture additional logins and passwords), or enable phishers to use the victim's computer to send out phishing e-mails to even more targets.

Not only have phishers refined their techniques, but also their attacks have grown more prevalent and costly. In August 2006, for example, 26,150 unique phishing attacks were reported to the Anti-Phishing Working Group, an increase of nearly 50% over the period 1 year earlier. *See* Phishing Activity Trends Report, August 2006, *available at www.antiphishing.org/reports/apwg_report_August_2006.pdf.* The number of phishing Web sites, corporate brands targeted in phishing attacks, and losses by consumers also have risen. The median loss per incident is now $850, up from just $165 in 2005, according to a recent survey by Consumer Reports magazine. *See* State of the Net 2006, *available at www.consumerreports.org/security.* And while phishing scams may cause considerable hardship to the individuals who find themselves victimized, they can also have a devastating impact on the institutions whose names are stolen in order to perpetrate these attacks. Not only do corporate victims suffer direct financial losses, such as reimbursements to defrauded customers, but they also face incalculable damage to their brands and reputations. It is clear that in order to preserve goodwill, protect their customers' accounts, and prevent the erosion of consumer trust in online banking, financial institutions must take proactive measures to thwart phishing.

Mark E. Plotkin is a partner and **Michael Epshteyn** is an associate, practicing in the Financial Institutions practice group of Covington & Burling LLP's Washington, DC, office.

Consumer Education

The critical event of every successful phishing scam is the phishing e-mail recipient's decision to click on an enclosed hyperlink. Indeed, most consumers could avoid becoming victims by simply ignoring phishing e-mails or deleting them from their inboxes. Thus, educating the public on how to identify and avoid phishing messages is the first step toward curbing phishing attacks. Raising consumer awareness will require the combined efforts of government, industry, and law enforcement. It will also be a constant challenge as phishing scams become more complex and harder to detect. Recent surveys have determined that most computer users cannot consistently distinguish fraudulent e-mails from legitimate messages. Still, there is a great deal that financial institutions can do to minimize the likelihood of their customers being duped by phishing scams.

First, financial institutions can educate their customers about the phenomenon of phishing. Although the concept of identity theft has entered the mainstream, the term "phishing" remains surprisingly obscure, and most consumers are unaware that it refers to the practice of stealing personal information through the use of sham e-mails. Corporate Web sites, while not alone sufficient, can be an excellent resource for teaching customers about phishing. Bank Web sites can explain phishing, offer tips for identifying scams, and even provide actual examples of the fake Web sites and fraudulent e-mails used in phishing attacks. Web sites can also inform customers that they will never be asked to follow an e-mail link to submit personal, financial, or account information.

Although Web sites can be an excellent resource, many individuals are unlikely to seek out, on their own initiative, information related to identity theft and phishing. Therefore, banks must take affirmative steps to alert customers to the threat. E-mailed security bulletins are one means of doing so; literature sent directly to the homes of customers is another. Federal regulators have even developed brochures that can be used in, or adapted for, banks' own customer-education efforts. *See, e.g.*, Office of Thrift Supervision, Phishing Brochure, *available at www.ots.treas.gov/docs/7/77437.html.* Other unconventional methods may also be needed. Some banks, for example, have recently begun to include warnings about fraudulent e-mails on the screens of their ATM machines. Banks will have to continue to experiment with these and other methods to determine how best to reach their customers and raise their awareness of online fraud. Striking the right balance, however, between delivering effective security warnings, on the one hand, and contributing to an erosion of trust in online transactions, on the other, will remain a significant challenge in the years ahead.

Secure Authentication

The popularity of Internet banking is in no small part attributable to the convenience and simplicity of conducting financial transactions online. Yet, it is the ease with which online banking customers can access their accounts — traditionally with nothing more than a user name and password — that makes Internet banking such a compelling target for phishers. Strengthening the customer authentication process — without unduly impacting customer convenience — is one of the central security challenges that financial institutions increasingly face.

The federal bank regulatory agencies have indicated that single-factor authentication (*ie*, user name and password) may, in their view, be insufficient to protect against phishing and other forms of online bank fraud. In October 2005, the Federal Financial Institutions Examination Council ("FFIEC") issued interagency guidance titled "Authentication in an Internet Banking Environment" ("Authentication Guidance"). *See* FFIEC, Authentication in an Internet Banking Environment, *available at www.ffiec.gov/pdf/authentication_guidance.pdf.* The Authentication Guidance, which supersedes 2001 guidance titled "Authentication in an Electronic Banking Environment," repeats the oft-mentioned three basic "factors" in authentication — namely, something the user *knows*, such as a password or PIN; something the user *has*, such as an

continued on page 3

Phishing

continued from page 2

ATM card or smart card; and something the user *is*, such as a fingerprint or retinal pattern — and states that "[t]he agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties." The Authentication Guidance calls for banks to consider shifting to multifactor authentication, yet does not require them to do so; instead, banks are expected to conduct a risk assessment of their online offerings, determine where the use of single-factor authentication is inadequate, and implement "multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks." In a detailed Appendix, the Authentication Guidance describes some of the authentication technologies and techniques that can be used to supplement a login/password-based system. These include:

- Passcode-Generating Tokens: Also known as "fobs" or "key fobs," these devices display a randomly generated passcode every 60 seconds, which matches a passcode being generated at the same time by software on the financial institution's authentication server. In order to access their online accounts, users must input their regular passwords and the correct randomly generated passcode.
- USB Tokens: USB tokens are small devices that plug directly into a computer's USB port in order to verify a user's identity. Once the USB token is recognized, the user is prompted to enter his or her password in order to gain access to the online system.
- Smart Cards: A smart card is the size of a credit card and contains a microprocessor that enables it to store and process data. A smart card must be inserted into a reader attached to the customer's computer. While they are relatively secure, and easy to carry and use, smart cards do require the installation of a hardware reader and associated software drivers on the user's home computer.
- Biometric Technologies: Biometrics encompasses technologies like retinal scanning, face recognition, voice recognition, and traditional fingerprint identification. It also includes the analysis of the rate and flow of physical movements, such as the pattern of data entry on a computer keyboard. Fingerprint technologies are the most mature and accurate of the various methods of biometric identification. However, much like smart cards, biometric authentication technologies typically require special hardware devices, and related software, to be installed on the user's computer.
- Scratch Cards: Analogous in principle to passcode-generating tokens, scratch cards are wallet-sized cards that, similar to bingo cards, contain numbers and letters arranged in a grid format. A customer attempting to access his or her account will be asked to enter, in addition to a password, the characters contained in a randomly chosen cell on the grid.

An authentication system that incorporates one of the above-listed technologies offers somewhat greater security than a system that relies solely on login IDs and passwords. The practicality of implementing true multifactor authentication, however, remains an open question. First and foremost, there is the issue of customer convenience. Customers expect to be able to access their accounts at any time and from any computer, which calls into question their receptivity to technologies requiring the installation of dedicated hardware and software, such as smart card readers and fingerprint scanners. In addition, even relatively hassle-free devices, such as passcode-generating tokens and scratch cards, obligate customers to carry an item that can be easily lost or misplaced. How will customers feel about being locked out of their accounts while waiting for a replacement key fob?

In addition to the burdens that would be placed on customers, a full-scale shift to multi-factor security would impose tremendous costs on banks, including upgrading and replacing existing IT systems, retraining service representatives, purchasing hardware tokens and other devices, and providing additional customer support. Nevertheless, despite legitimate concerns over cost and convenience, the very real threat posed by phishing and other forms of online fraud will compel banks to adopt forms of authentication that go beyond simple password entry. Fortunately, there are a number of authentication methods that offer more security than basic password access, yet are less burdensome and less costly than full-fledged multifactor authentication. These "single factor plus" solutions rely primarily on what a customer knows, yet also emulate, to a certain extent, what customers have (the second factor in true multifactor authentication).

For example, there are software products that enable a financial institution to create an "access signature" for each customer by collecting and analyzing data such as IP addresses, domain names, and customary login times. If a user with a nonmatching signature attempts to access a customer account, the bank can either deny access or ask a series of "challenge" questions that would be difficult for anyone but the customer to answer correctly. Other "single factor plus" methods include geo-location technology (in which Internet communications are analyzed to determine the physical location of a user) and the placement of encrypted "cookies" on customers' Internet browsers. These allow a bank security system to raise additional barriers to entry when it detects that a customer is attempting to log in from a new geographic location or from an unverified computer. Yet another potentially promising authentication technique is the use of "shared secrets" to identify the financial institution's Web site to the user. In a typical scenario, a customer will be asked, when establishing his or her online account, to select an image from a group of stock photographs (or, alternatively, to upload an image of his or her choosing). In the future, whenever that customer logs in to the company's site, the selected image will be displayed, letting the customer know that he or she is accessing the genuine site.

continued on page 4

Phishing

continued from page 3

The preceding enumerates only some of the many methods available to authenticate customers' identities online. As new techniques are developed, financial firms will have to balance the need to guard against Internet fraud with customers' demands for fast and easy Web-based access to their accounts. While the ultimate solution to this challenge remains unclear, it is becoming increasingly apparent that firms will have to go beyond traditional single-factor authentication to provide adequate security in today's online world.

Conclusion

Phishing represents a genuine threat to the security and integrity of online banking, and one that is likely to increase in severity and sophistication over the years to come. Although there is no instant solution, financial institutions can reduce the risks of phishing by raising customer awareness of online fraud and implementing strengthened user authentication systems. While many banks are technology leaders in the fight for online security, there also are many other financial institutions that are falling behind, as phishing's sophistication grows ever greater. In order to preserve consumer confidence in the online banking sector, it will be necessary for the vast majority of financial institutions to adopt a forward-looking policy of continuing innovation and enhancement in the battle against phishing.

—❖—