



Legal Perspectives

FFIEC Issues New Guidance on Authentication in Online Transactions

By Benjamin S. Hayes and Jeffrey B. Ritter

On October 12, 2005, the Federal Financial Institutions Examination Council ("FFIEC")¹ issued guidance entitled "Authentication in an Electronic Banking Environment" regarding authentication of customers in online financial transactions. This guidance updates guidance issued in 2001 and states three essential points:

- ▲ Single-factor authentication, as the only control mechanism, is considered inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties;
- ▲ The authentication techniques employed by the financial institution should be appropriate to the risks associated with the involved products and services; and
- ▲ Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multi-factor authentication, layered security, or other controls reasonably calculated to mitigate those risks.

The new guidance requires compliance by December 31, 2006.² Many financial institutions offer their customers the ability to perform online transactions using only single-factor authentication. Thus, banks and other affected financial institutions face a delicate balancing act—strengthening their authentication processes while maintaining the user-friendliness of their online facilities and containing costs.

The FFIEC identifies three factors as driving the need for new guidance: legal and technological changes regarding the protection of customer information; increasing incidents of fraud, including identity theft; and improved authentication technologies. While FFIEC guidance is neither law nor regulation, it determines the standards by which certain financial institutions are examined by regulators. Institutions that are found not to comply with FFIEC standards can be sanctioned by their regulators. The new FFIEC guidance builds on a study issued by the Federal Deposit Insurance Corporation in December 2004 entitled "Putting an End to Account-Hijacking Identity Theft," and supplemented by a February 2005 addendum.

Options For Authentication In Online Banking

A common means of authentication in the online banking environment is the use of a user ID and password that are known only to the customer and the financial institution. ATM transactions commonly require two-factor authentication because they require the use of an ATM card (something the person has) and a PIN (something a person knows).

While the terms "single-factor" and "two-factor" (as well as "double-factor" and "multi-factor") are generally used to describe layered authentication processes using more than one category of authentication, "multi-factor authentication" is also sometimes used to refer to authentication based

solely on layers of a single category (such as what a person knows), if the different layers are implemented in different ways. Examples include:

- ▲ Reverse Authentication—a process by which the person being authenticated also authenticates the identity of the financial institution. For instance, a customer might select an image when he or she signs up for online services, and then during a sign-in process that image is displayed to the customer to provide assurance that the Web site really is the financial institution's site. The customer supplies the customer's ID and the customer's recognition of the image.
- ▲ Out-of-Band Authentication—authentication by a separate communication channel, other than the one on which a transaction is initiated. An example of out-of-band authentication is an automated telephone call to a customer being generated during an online authentication process.
- ▲ Challenge and response regarding the customer's identifying information. Examples are queries regarding last 4 digits of the customer's social security number or date of birth.
- ▲ Challenge and response regarding information supplied by the customer. Examples are queries regarding pet's name, name of high school or color of first car.

Other Controls

The new FFIEC guidance is not focused exclusively on authentication. It explicitly refers to "other controls reasonably calculated to mitigate" the new risks associated with online transactions. An example of another control is an automated process by which information is encoded as it is entered. At least one major online bank has introduced a process whereby the customer is presented with numbers on a virtual keypad that also features letters. The customer must use a mouse to click on the numbers of the customer's PIN, which generates a letter code that is communicated to the server. The precise letters associated with each number change constantly and are synchronized with the server, the result being that although the customer enters the same information each time he or she logs in (i.e., his or her PIN), the actual data passing between the customer's computer and the bank's server is a constantly changing passcode. While the information being entered is authentication information, the essential effect of this process is to reduce the likelihood that the customer's PIN will be captured in transmission.

Compliance Process

The FFIEC expects each financial institution to approach compliance with the new guidance in three stages:

- ▲ Identify and assess the risks associated with its Internet-based products and services.

- ▲ Assess the adequacy of authentication techniques and adjust its information security program.
- ▲ Implement appropriate risk mitigation strategies.

Possible Risk Mitigation Strategies

The following are three general strategies that financial institutions can use to meet the FFIEC's new standards for online authentication:

- ▲ Uniform procedures that require multi-factor authentication for all online customers, regardless of the type of transaction the user accesses the Web site to perform.
- ▲ "Zone" based authentication. Under this approach, accessing informational features or account balances requires minimal authentication, accessing customer profile information or paying bills require a higher level of authentication, and fund transfers to third parties or account liquidation require the highest level of authentication.
- ▲ Per-transaction risk assessment. This approach uses sophisticated software to assess the risk index associated with each individual transaction in real time and assign a degree of authentication based on a risk score.

Each of these strategies has its relative costs and benefits. Uniform procedures could result in an increased burden on customers who use online services only or principally for low-risk transactions such as checking account balances or interest rates. Zone based authentication may provide an easier sign-on process for customers seeking only information, but may require costly partitioning and re-programming of online services. Per-transaction risk assessments are likely to produce the most user-friendly customer experience, but require the use of expensive software and may result in banks' dependence on particular software vendors.

Possible Outcomes

Anecdotal evidence suggests that U.S. banks may resist implementing authentication processes that are, strictly speaking, two-factor authentication because of the relatively higher costs associated with tokens and biometrics. Instead, banks may rely more heavily on multiple layers of a single type of authentication—what the customer knows. Reverse authentication and out-of-band authentication may increase in popularity because they

also rely on what the customer knows and thus generally do not require additional hardware.

Per-transaction risk assessment software may ultimately be adopted on a widespread basis because it offers the greatest flexibility and promises to reduce the burden on the customer to the greatest degree possible. It is also significantly less expensive than distributing tokens to an entire customer base, capturing biometric data for an entire customer base, deploying all the associated new hardware, and administering both systems. Biometrics may also not be widely adopted because of a concern that customers may perceive such measures as onerous or invasive and gravitate to other financial institutions that do not require such procedures.

Finally, it seems likely that, as multi-factor authentication becomes more prevalent in the financial services industry under regulatory compulsion, these processes will become more widespread in other industries and in the lives of Americans generally. While initially required only of entities regulated by FFIEC member agencies, these procedures seem likely eventually to be expected of other types of financial institutions (for instance, broker-dealers or insurers).

Implementing The Legal Aspects

When financial institutions implement multi-factor authentication, attention should be paid to legal considerations such as the following:

Acquiring New Technologies. When new authentication technologies are acquired, the related purchase or licensing agreements provide an opportunity for institutions to consider and allocate some of the new types of risks associated with those technologies. For example, biometric technologies, which require the capture and storage of new identifying data, may justify special terms regarding warranties, security controls, and allocation of liability in the event of service failures.

Customer Service Agreements. Existing customer service agreements may require amendment in order to obtain the consent of customers to the new authentication methods. In addition, terms addressing limitations of liability should be examined in order to confirm that those terms work effectively with the potential liabilities presented by the new authentication technologies.


Privacy Policies. Various authentication technologies can involve the capture of additional personal information or different uses of personal information that has already been captured and stored by a financial institution. Existing privacy policies may require revision to accommodate these practices; of course, these revisions may be

accomplished in many instances concurrently with related customer service agreement revisions.

Variable Risks. Many institutions adopt a uniform view of electronic transactions, implementing similar procedures and authentication controls for transactions with widely varying economic value and risks. As part of the required risk assessments, financial institutions may conclude that different Web site terms and conditions are appropriate based on the nature of the transactions with which the new authentication methods will be employed.

Precise Standards Unclear

The main problem many financial institutions may encounter in seeking to comply with the FFIEC guidance is that the guidance provides very few defined standards. It requires that authentication and other anti-fraud measures be commensurate to risks identified during a risk assessment process, but provides few clear metrics on when multi-factor authentication will be called for. For instance, the guidance states "authentication techniques employed by the financial institution should be appropriate to the risks associated with those products and services," but fails to define "appropriate" in a meaningful way. The guidance provides that single-factor authentication is "inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties," but does not clarify whether this means access to *any* customer information (e.g. account balances) or only sensitive information such as social security numbers or home addresses.

It can reasonably be anticipated, therefore, that there will be some degree of confusion as the compliance date approaches. Security professionals who are called upon to implement the FFIEC standards for financial institutions are well advised to participate in industry forums, refer to developing international standards, and keep track of what other financial institutions are doing. 

Benjamin S. Hayes and Jeffrey B. Ritter are attorneys in the Washington, DC office of Kirkpatrick & Lockhart Nicholson Graham LLP.

¹ The FFIEC is composed of the Board of Governors of the Federal Reserve Board System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, and the National Credit Union Administration. The FFIEC was established in March 1979 to prescribe uniform principles, standards, and report forms and to promote uniformity in the supervision of financial institutions.

² See FDIC FIL-103-2005 and OCC Bulletin 2005-35, both also dated October 12, 2005.

Note: This article does not contain or convey legal advice. The information herein should not be used without first consulting a lawyer.