THOMSON REUTERS

Westlaw®

Electronic banking: Risks and requirements

By Scott Sargent, Esq., *Baker Donelson*

DECEMBER 10, 2018

Electronic banking has become part of everyday life. Many consumers receive their compensation, pay their bills and move their money using only their personal devices or computers. In the United States, literally billions of dollars are moved every day with nothing more than a than a few clicks or touches on a screen. Unfortunately for banks, they bear the risks involved in these transactions from the inception of the relationship with the customer until the account is closed.

While the risks of electronic banking are significant, they are manageable if a bank identifies them and develops and implements mitigation controls and processes. It is imperative that banks frequently take time to consider risks and evaluate their exposure. With that in mind, some of the more significant risks that banks should account for in their electronic banking strategy are discussed below.

BANK SECRECY ACT/KNOW-YOUR-CUSTOMER RISKS

The Bank Secrecy Act and anti-money laundering requirements for online banking are intended to keep banks from conducting business with prohibited individuals and entities, including terrorists. In the context of online banking, these requirements become a bit more complicated.

While the risks involved in electronic banking are significant, they are manageable if a bank identifies them and develops and implements mitigation controls and processes.

Primarily, the bank has a duty to know its customer. In the traditional banking relationship, that is easily achieved through in-person verification utilizing established documentation. With respect to online account origination, where the individual may never be seen by a bank employee, it is more difficult.

There are established vendors that can verify a customer's online identity with impressive accuracy, but those services represent a hard cost to the banks. Financial institutions may also utilize technology to verify identity via biometrics, video conference, telepresence or through the process recently authorized by the MOBILE Act. Under the statute banks can take electronic copies of state issued driver's licenses or identification cards to verify identity without violating state laws.

In any case, appropriate due diligence, internal controls and employee training are required to manage the BSA/KYC risks associated with electronic banking. The implementation of appropriate policies, procedures and processes should provide risk mitigation and security while still meeting the online onboarding needs of the customer.

OPERATIONAL RISK

Operational or transactional risk arises from errors, system failures or other events that impair an institution's ability to deliver products or services. For electronic transactions, this risk is complicated by customer demands and the speed at which banks and financial technology companies are innovating and expanding the reach of online banking. The customers' expectation that electronic banking be available at all hours, every day means that banks must have systems and capacity to ensure reliability and accessibility.

It is imperative that banks have policies, procedures and controls in place to address the risks inherent in electronic banking operations. Information security controls are essential to a bank's enterprise risk management system, but electronic banking specifically requires additional tools, expertise and testing. The necessary level of security controls should be based on the bank's risk tolerance aligned with the products offered and transaction volume.

FRAUD RISK

Online banking fraud costs financial institutions and their customers millions of dollars every year. It is an inevitable risk that a customer's online banking credentials will be compromised or stolen. As a result, state and federal authorities have implemented specific legal and regulatory requirements for financial institutions so they can protect and educate their customers. These requirements protect the banks as well. Generally, banks are required to:

- Perform annual online banking risk assessments — it is important to identify those accounts or account types that may be most susceptible to fraud and implement appropriate controls to mitigate potential losses.
- Implement layered security controls, including multifactor authentication for higher-risk transactional online banking services, and examine available security controls that could be or should be implemented.

- Consider additional security requirements for online banking account administrators. In some cases, it may be appropriate to make some security procedures mandatory, such as dual control and/or out-of-band confirmations, which require the active involvement of multiple people or multiple verifications to complete a funds transfer. Dual control can be as simple as having someone other than the initiator verify the transaction. Out-of-band confirmations involve two-factor authentication and transaction authorization through a separate communication channel.
- Regularly communicate information regarding security best practices and emerging security threats to customers.
- Establish firm transaction exposure limits for customers based on their credit and account histories.
- Implement monitoring processes that identify anomalous transactions.

Banks must also remain aware of the requirements of Article 4A of the Uniform Commercial Code. This UCC framework includes a description of how a payment order will be considered authorized and verified, and this process is based on a security procedure's commercial reasonableness. Commercial reasonableness of a security procedure is generally determined by considering:

- The size, type and frequency of payment orders normally issued by the customer to the bank.
- Alternative security procedures offered to the customer.
- Security procedures in general use by customers and similarly situated receiving banks.

A security procedure will also be deemed commercially reasonable under Article 4A if both of the following requirements are met:

- The security procedures utilized in the transaction were chosen by the customer after the bank offered, and the customer refused, a security procedure that was commercially reasonable for that customer.
- The customer agreed in writing to be bound by any payment order, whether or not authorized, issued in its name and accepted by the bank in compliance with the security procedure chosen by the customer.

This provision is very important when banks have customers, particularly large commercial customers with high transactional volume, who decline to implement suggested security enhancements. The bank should always memorialize in writing any customer's refusal of a security enhancement or procedures in accordance with Article 4A.

In disputes over liability for unauthorized transactions, many courts determine whether a security procedure is commercially reasonable by combining the analysis of Article 4 of the UCC with applicable regulatory guidance.

LEGAL AND COMPLIANCE RISK

Electronic banking and electronic transactions present new and different legal and compliance risks as well. In many cases, electronic banking involves additional laws and rules that are not applicable to traditional banking. Some of the specific legal and compliance risks that should be considered in electronic banking are:

- Jurisdictional issues that may affect a given transaction (federal law, state law or foreign law).
- Delivery and acceptance of required disclosures.
- Contract formation.
- Document retention and delivery for services offered online or via ATM (advertising, disclosures, notices, agreements).

The Bank Secrecy Act and anti-money laundering requirements for online banking are intended to keep banks from conducting business with prohibited individuals, entities and terrorists.

Many regulations relate to certain circumstances or types of transactions and may require specific actions, processes, procedures and infrastructure from the bank. Some of the regulatory requirements that could or do specifically relate to electronic banking include:

- A consumer's right to dispute electronic transactions and the bank's required response and investigative actions (Regulation E and Regulation Z).
- The collection and reporting of government monitoring information on loan applications and loans as required by the Equal Credit Opportunity Act (Regulation B) and the Home Mortgage Disclosure Act (Regulation C).
- Advertising requirements, customer disclosures or notices required by the Real Estate Settlement Procedures Act, the Truth in Lending Act (Regulation Z), the Truth in Savings Act (Regulation DD) and the Fair Housing Act regulations.
- Proper and conspicuous display of Federal Deposit Insurance Corp. insurance notices.
- Delivery of privacy and opt-out notices pursuant to the Gramm-Leach-Bliley Act and Regulation P.

- Verification of customer identification, reporting and record-keeping requirements under the Bank Secrecy Act, including requirements for filing a suspicious activity report.
- Record retention requirements of the Equal Credit Opportunity Act (Regulation B) and Fair Credit Reporting Act regulations.

Both informational and transactional electronic banking services have an increased compliance risk because of the lack of in-person verification for transactions, the speed at which technology changes, the instantaneous nature of online transactions and the frequent changes to regulatory requirements made to addresses electronic banking concerns.

REPUTATIONAL RISK

Finally, a bank can never ignore the potential impact electronic banking can have on its reputation. The news is replete with stories about data breaches, online hackers and stolen identities. Bank customers and regulators expect online transactions to be completed seamlessly and securely. A bank's failure to meet those expectations can result in significant damage to its reputation. A bank's reputation can be damaged by any or all of the following:

- A data breach that compromises customers' financial information.
- Unauthorized/fraudulent activity on customers' accounts.
- System failures resulting in service disruptions.
- Failure to deliver on product performance representations.
- Customer complaints.

CONCLUSION

In today's digital world, everyone expects to be able to order groceries, pay their phone bill or send money to their kids at college with little effort and maximum security. It is incumbent on banks to recognize the risks involved in these transactions and manage them accordingly. In most cases, it is a matter of simply considering the risks of electronic banking broadly, analyzing the risks of each service or product offered and mitigating those risks according to the bank's risk profile and appetite.

When the risks are identified and controlled appropriately and the infrastructure exists to maintain vigilance, both the customer and the regulators will know the bank's electronic transactions are as secure as possible.

This article first appeared in the December 10, 2018, edition of Westlaw Journal Bank & Lender Liability.

ABOUT THE AUTHOR

Scott Sargent is an attorney in **Baker Donelson**'s Birmingham, Alabama, office, where he advises community, regional and international banks on regulatory compliance and risk management. As part of his banking practice and work with financial technology companies, he helps his clients implement regulations and best practices concerning data security, privacy and protecting confidential information. He can be reached at ssargent@bakerdonelson.com.