Synopsis: There are at least 18 regulations affected by Wireless Banking that the Federal Financial Institutions Examination Council's (FFIEC) defines as banking activity conducted over a wireless telecommunications network (like cellular, 3G, or 4G networks). From restructuring the bank's E-banking Policy to making sure vendors facilitate the compliance processes to arranging for the distribution of disclosure statements after-the-fact, the risks associated with Wireless Banking are many, but controllable. This article delineates 5 steps that a Compliance Officer should take to prepare for Wireless Banking.

Step One: Understand the basics of wireless banking.

Step Two: Restructure the E-banking Policy into a Branchless Banking Policy.

Step Three: Insist upon strong Vendor Due Diligence.

Step Four: Create a Risk-based flexible deployment strategy.

Step Five: Using the Branchless Banking Policy, apply each regulation to your selected deployment strategy.

Five Steps to Wireless Banking Compliance

The hope is that the guidance specifically addressing Wireless Banking, dated 2003, will be updated soon. We know that Wireless Banking will be the subject of future compliance audits and examinations.

Which regulations are affected by Wireless Banking? The short answer: all of them.

Or at least 18 of them.

The same regulations that are considered in your existing E-banking Policy must be considered. In addition, Wireless Banking touches regulations not covered by most E-banking policies because they cover transactions traditionally handled in the branch.

As we watch management warm up to adoption, compliance needs a starting point. Given Wireless Banking's untested complexity, coupled with an overwhelming number of affected regulations, the task of ensuring compliance might seem daunting. But let's reduce the process to five steps.

Step One: Understand the Basics of Wireless Banking

Most believe the adoption of smartphones will be classified as a revolution in The History of the Information Age. Smartphones intuitively allow us to do anything we want, anywhere we want, any way we want. This makes them the ultimate in convergence, convenience, and customization.

Though mostly referred to as "mobile banking," the act of allowing customers to bank with hand-held devices connected via cellular, 3G, or 4G networks, is called "Wireless Banking," in the FFIEC's E-banking Handbook, Appendix E. Dated 2003, this appendix is the last known guidance on the subject; a subset of what the FFIEC calls "Branchless Banking."

We can reduce Wireless Banking to three "channels." Most institutions already have the Mobile Web Channel, a version of your on-line banking site, reformatted for the smaller screen size of older, web-enabled "dumb phones." (Treo, BlackBerry Pearl, Samsung Messager, etc.).

Most on-line banking sites recognize a cell's browser request and redirect the browser to m.mybank.com or mybank.mobi sub-sites. More sophisticated mobile web deployments are streamlined for the type of activities conducive to the cell. For example, the mobile web experience downplays data input transactions, and instead allows us to check balances, monitor transactions (such as cleared checks or deposits), and authorize payments to existing payees. Though this functionality rises from the cause of convenience, it also supports risk mitigation.

The second channel is SMS or Text Banking. One-way text banking allows text messages from the bank, based on user-defined thresholds. The texts include real-time information such as balance alerts, transaction alerts, and out-of-band passwords. Two-way SMS banking allows users to text inquiries and transaction orders. SMS banking comes with many risks including smishing and intercepted text messages.

The hype surrounding Wireless Banking centers around the Mobile Application Channel, made possible by a "marketplace" maintained by the platform provider. The two most prevalent American platform providers are Apple (with the iPhone's iOS), and Google (with the Android operating system).

The Mobile Application Channel provides traditional on-line banking functionality more conveniently than the Mobile Web channel, but also offers opportunity for creative banking transactions including Consumer Capture (take a picture of a check to deposit it), stock trading, complaint submission, secure messaging, marketing, Mobile Payments (pay for goods with your smartphone), and peer-to-peer (P2P) payments (transfer money to a friend's smartphone). The latter two combine with other non-bank applications such as PayPal or Starbucks Gifts to be part of what we call "wallet capabilities."

Typical tension between marketing and compliance arises with the opportunities afforded by New User Registration. Marketers want to allow users to download the bank's application and immediately begin bank interaction (or at least fill out marketing surveys tied back to the CRM package). Obviously, many regulations are affected by this activity. Simply disallowing New User Registration (or requiring it from established delivery systems) makes compliance much easier, but misses one of the important benefits sold during the persuasion phase of adoption: new customers.

Beyond the "three channels" of Wireless Banking, we must also consider the "Prevalent Platforms" in the smartphone market, as well as "Non-traditional Feature Adoption." When we consider Prevalent Platforms, we address the strategic risk of creating an application (and all the service peripherals) for a platform that eventually loses the market share war between smartphone providers. In America, the iPhone platform (iOS) and the Android platform (Google) seem stable. The BlackBerry 6 OS platform (Blackberry Torch, Style, Bold, etc.) and the Windows Mobile platform (Samsung Focus, HTC Arrive, and many others), though promising, still present strategic risk as we do not know for sure if they will be adopted.

The key difference between Wireless Banking and On-line Banking is what we call "Non-traditional Transaction Capabilities" of the smartphone applications. These capabilities mostly center around a "wallet feature" of the smartphone. The many competing methods to transfer money from the smartphone application's wallet to the retailer's cash drawer . . . "Scan and Pay" and "Wave and Go" are examples . . . create strategic risk in our adoption of these features because, like non-prevalent platforms, we can not know which method will become a stable standard. We can transfer this risk to our vendors. Otherwise, we must wait to see which payment methods retailers adopt before we commit fully to any one standard.

Step Two: Restructure Your E-banking Policy

To prepare for Wireless Banking, consider overhauling your E-banking Policy. The structure of most E-banking policies originally addressed ATMs and telephone banking as well as new payment processing technologies such as electronic wire transfers and electronic funds transfers. As new delivery systems, payment processes, and authentication solutions became available, many E-banking policies evolved into a collection of after-thoughts trying to address new technologies as they emerged.

Consider replacing the policy with a “Branchless Banking Policy” structured around three primary asset categories: Payment Processes, Delivery Systems, and Authentication Solutions. Each asset category would then include the various assets the bank has adopted, and each asset would then address strategy, risk management, applicable laws and regulations. We have revised our own boilerplate for this purpose, which is available for free at m.infotex.com/mobilerisk.

Step Three: Insist Upon, and Become Involved With, Strong Vendor Management

The bad news? If you intend to truly leverage the differences between On-line and Wireless banking, and thus offer functionality including New User Registration, Wallet Capabilities, and Consumer Capture, you will not always be able to rely on existing on-line banking practices for your “compliance response.”

The good news? For several years now, we have been improving our vendor management practices. These efforts were often resisted, and compliance was often the driving force in these improvements. With Wireless Banking, these efforts will pay off. All normal compliance processing arising from a bank transaction may need to be designed into the smartphone application. Thus, the most effective way to mitigate compliance risk is with strong vendor due diligence. A free vendor due diligence kit at m.infotex.com/mobilerisk will get you started in asking the right questions.

This kit includes a checklist of questions with risk-ranking capabilities as well as a list of alternative vendors. Your existing on-line and/or core provider does make a viable option, and does provide some economies (for example, you don’t have to pay for a brand new infrastructure if you use your existing provider). But third-party providers have a lot to offer, will respond to price pressure, and may be willing to share in some of the strategic risk. Now is the time to dust-off the Request for Proposal (RFP) procedure and cast a wide net.

Because compliance processing is dependant upon the way the application is designed, vendor statements like “ultimately compliance is the bank’s responsibility” should not be accepted. While of course we agree with this statement, we see some vendors who help bankers develop their compliance processes, and some vendors who don’t. But the bank can’t design the application to track GPS positions and feed that information into anomaly monitoring applications. Likewise, the bank can’t design the application to restrict high-risk transactions, or to automatically check MICR codes during consumer capture to prevent duplicate deposits.

If the bank opts for New User Registration, not only must the database have controls over which fields must be populated prior to allowing certain transactions, but the application, and not the bank, will need to facilitate disclosures. Disclosure requirements abound with Wireless Banking. The application design, not the bank, must overcome disclosure and message limitations. If the application allows one to check rates, then the application must allow the bank to provide the Reg. Z disclosures in cell-size formatting.

Thus, the vendor due diligence process must involve the Compliance Officer. It’s that simple.

Regulators will wait for you to design your compliance response to Wireless Banking issues before they weigh in on what could and should be done. If it is obvious that compliance was considered organically during selection and deployment, you will be in a good position.

When banking required new customers to come to the branch, smaller community-based banks thankfully didn't have to worry too much about terrorists and the Counter Terrorism Financing (CTF) regulations. But if account origination starts by downloading an application from anywhere in the world, we better be sure our application developers have carefully matched which database fields must be populated before we can allow transactions that would violate the Counter Terrorism Financing regulations.

Tension between convenience and security surfaces in decisions about the authentication process used to access wireless banking services. If you want convenience, you'll increase your risk exposure over two-factor, strong authentication. Again, these are all choices made during vendor selection. Compliance must be involved.

Under the E-SIGN Act, to obtain effective consumer consent to receiving electronic disclosures, financial institutions must, among other things, inform consumers of the hardware and software requirements for retention of electronic records that will be provided as disclosures. Will your application handle this? What if you allow customers to register from their smartphone? How do you get these disclosures to them? These requirements should be carefully considered by a team that includes your technology professionals, information security professionals, and of course your compliance staff.

Step Four: Create a Risk-based Flexible Deployment Process

A barrier to adoption has always been the risks associated with Wireless Banking. Unlike the home computers used with on-line banking, we can lose our cell phones in social functions, shopping malls, vacations, etc. We have identified over forty different vulnerabilities specific to Wireless Banking. Financial institutions have experience mitigating security and compliance risk, but Wireless Banking will require a strong strategy planning component to mitigate strategic risk.

Financial institutions that are successfully deploying Wireless Banking mitigate strategic risk by having a long-term strategy governing flexible short term tactics. They start in all three channels, and then focus on one platform at a time. They pay close attention to the consumer electronics press when they look down the road. But this year? They have a regular schedule of what they're rolling out, taking it one step at a time.

For example:

- Now: Mobile Web (m.ourbank.com or ourbank.mobi)
- Next Month: SMS
- The Following Month: iPhone App
- And the Month After That: Android App; Scan and Pay on both apps
- Sooner or Later: Consumer Capture??
- The Rest of 2012: Possibly new platforms (such as Blackberry RIM or Windows Mobile) or new features.

The tactical plan can change as the year progresses, but the help desk must be well-trained on the short-term tactical objectives. Each phase of deployment formally ends with a confirmation phase, a “post-mortem” analysis, and an update of all compliance documentation. The next phase begins with an update of the risk assessment and the Branchless Banking Policy.

Step Five: Using the Branchless Banking Policy to Test your Selected Deployment Strategy
If you adopt the proposed restructuring of your E-banking Policy as described in step one, you now have a map to test your deployment strategy. The new structure is asset-based, and thus as you choose deployment options presented by your vendor, you will want to assign them to an asset or asset category. Within each asset, be it a payment process, delivery system, or authentication solution, the following would be addressed as appropriate:

- Strategy: This is where you would document your phased platform adoption strategy and other strategy-related issues (such as ways to transfer strategic risk to the vendor).

- Risk Management: Revisit and update your initial risk assessment, monitor development of controls, document lessons and obligations determined in the vendor due diligence process, and test against data security objectives. Be sure to consider and document record retention strategies, legal risk mitigation strategies, and compliance concerns. All applicable laws and regulations must be tested.

Our policy template lists all 18 applicable laws and regulations. To illustrate how this works, let’s briefly cover each applicable law and regulation from A to Z:

- Applicable Laws:
    - Americans with Disabilities Act (ADA): We would like to think that the smartphone design itself will accommodate the Americans with Disabilities Act, but then we thought that way about our ATMs, didn’t we? It wouldn’t hurt to bring this up during vendor due diligence.

    - BSA / AML: Some predict that small business owners, professionals, and famers will join Millennials in adopting Wireless Banking because of the Consumer Capture feature. If you offer it, you will want to be sure appropriate reviewing, flagging, and reporting does not get missed by the way the mobile application integrates with your existing compliance processing systems. The standard questions (when, where, how and who) need to be supplemented during vendor due diligence with questions about how the application integrates with your core. Does it compare MICR codes with previously deposited checks? Meanwhile, is the consumer required to maintain a copy of the check and for how long? See UCC Article 4A for commercial accounts, and the advice of your vendor and existing compliance responses for consumer accounts.

    - CAN-Spam Act: If we choose to use the secure messaging and text messaging capabilities of Wireless Banking to deliver marketing messages, we must be sure to consider this law. All the nuts and bolts related to do-not-call lists, opt-out features, and disclosures may or may not apply, depending upon your approach. How will you fit the CAN-Spam signature and a marketing message in the restricted message length?

    - Counter Terrorism Financing (CTF): See USA Patriot Act.

    - Electronic Funds Transfer (EFT) Act: See Regulation E.

- E-Sign Act: Beyond the uncertainty surrounding voice recognition, there are a lot of other issues impacted by this law. If your customer wants to transact business requiring disclosures, they must first agree on electronic delivery of disclosure statements. The bank then has to extend the disclosures in the electronic format (usually an e-mail of a PDF), and then the customer has to confirm they have the ability to receive the e-mail via their smartphone, and then the ability to read the PDF on their smartphone. If you already have e-mail disclosure approval from on-line banking, you should be okay for wireless banking as long as you still use the e-mail channel.

  Signature cards must also be addressed. Your initial contract must specify your approach on signature cards and secure your customer's agreement to its provisions. Some banks are treating an image of the first documented customer signature as a temporary signature card. The theory is to open the account temporarily with limited transactions and amounts, and invite the customer to come into the branch before more complex, higher risk, or additional low-risk transactions are allowed. Regardless of how you treat it, as the signature card is technically an agreement, the process you choose might need to be reviewed by your legal counsel.

- FACTA (and the Red Flags Rule): If you are going to allow new user registration, the key question becomes: What red flags at point of purchase in retail banking or in on-line banking need to be translated to the Wireless Banking reporting system? The checks related to consumer credit reporting should not be affected, but how does the bank address those questions related to suspicious personal identifying information? And how will you establish patterns of activity in the account? These questions should be asked during vendor due diligence.

  You might be tempted to think that since the application ties to the core and these reports are run from the core, you should be okay. But the real question then becomes: are all fields in the mobile application properly mapped back to the core? Are we getting all the information to the core that we would normally expect? And what information do we process outside the core to facilitate the Red Flags program? How is that information collected, and will the mobile application need to collect this information?

- Gramm-Leach-Bliley Act (GLBA): Beyond the vendor due diligence already established in this article, and the 40+ questions related to security that are inherent in the free template for a Wireless Banking risk assessment (m.infotex.com/mobilerisk), the bank needs to be very careful about ensuring that the results of your risk assessment do not get lost in the many other to-do's related to deployment. Meanwhile, do you have a plan to check for application security audits and how do you know what a good audit looks like? And how do you do your own testing to confirm basics such as encryption of account information and authentication credentials on the smartphone? A call to your IT audit firm may be in order.

- Office of Foreign Assets Control (OFAC): See USA Patriot Act.

- UCC Article 4A: If the early majority adopters are truly going to be professionals (doctors, lawyers, etc.), small business owners, and farmers (the theory is they'd all be interested in consumer capture and other alerting features of Wireless Banking), then UCC Article 4A should be considered because Regulation E applies to only the consumer. Remember, remote capture (and by extension consumer capture) is just another way to deposit money. For commercial businesses, UCC Article 4A requires the commercial customer to maintain the actual check.

- USA Patriot Act (CIP and KYC, CTF): If a big part of the adopt-now decision is based upon the marketing opportunity of New User Registration, you must consider the implications of this on your Customer Identification Program (or Know Your Customer or Customer Due Diligence). Smaller banks that may have escaped these issues as a primary compliance priority might need to revisit the issue due to the fact that a terrorist now has access to the bank's front door through the Google or iPhone marketplace. The standard answer I'm hearing is "manage the risk by allowing the application to be downloaded and allow for 'basic transactions' but nothing more until the user comes into the bank to 'populate the database.'" When it comes to new user registration, the U.S. Patriot Act, OFAC, and CTF will be impacted the most. The OFAC list will need to be checked, but when? Can it wait until after the new user comes into the bank to "populate" the unpopulated database?

- Applicable Regulations:

  - Regulation B, Equal Credit Opportunity: If we use Wireless Banking for marketing purposes (such as a threshold for "text me when your interest rate reaches 4.5%") we must remember to include all the disclosures, which relates directly back to the E-sign act for delivery method.

  - Regulation C, Home Mortgage Disclosures: Anytime the mobile application assists with credit processing (ranging from origination through monitoring), Regulation C will be affected. Even a credit facility linked to the deposit account or overdraft line of credit will require the same consideration as a home equity line of credit, which would be impacted if tied to the "wallet capabilities" of the application. Your compliance response shouldn't be any different than on-line banking, other than the use of the asset might proliferate with smartphone applications. Of course, as with other regulations, delivery of disclosure statements may be problematic.

  - Regulation CC, Availability of Funds and Collection of Checks: You will need to revisit this regulation if you roll out the Consumer Capture and/or P2P capabilities of smartphone applications. Will you put a hold on a check until funds are confirmed? And how are you going to confirm funds on a P2P transaction?

  - Regulation DD, Truth in Savings: I'm trying to imagine a situation where a millennial would want to set up a savings account over the smartphone. But if you choose to offer saving accounts over the smartphone, it would be far better to find out during vendor due diligence that your response to this regulation includes proper disclosures that must be delivered prior to the first transaction.

  - Regulation E, Electronic Fund Transfers: The regulation that establishes the rights, liabilities, and responsibilities of parties in electronic funds transfers definitely impacts Wireless Banking, exposing your bank to liability under Reg. E for unauthorized activities if a customer's smartphone is lost or stolen. The risk exposure is a function of the products, services, and capabilities you are providing through your mobile banking application. For example, the loss of a smartphone used to conduct transactions would be similar to losing an ATM or debit card with a personal identification number written on it. However, the risk to the institution may be greater depending on the types of Wireless Banking services offered (e.g., bill pay, person-to-person payments, mobile payments, etc.) Not only will Wallet Capabilities such as "Scan and Pay" have Reg. E implications, the bank should be prepared for an increased number of disputes related to liability. It might behoove you to bring this up in your next insurance review.

- Regulation M, Consumer Leasing: See Regulation C.
- Regulation Z, Truth in Lending: See Regulation C.

Yes, that was 18 regulations. Yes, Wireless Banking reeks of risk. Yes, it touches upon almost every regulation related to banking. And yes, if compliance inserts itself in the vendor due diligence process, deployment will be smoother and less costly. A team of motivated technology, marketing, security, and compliance personnel can rise to the challenge!

DAN HADAWAY CISA, CISM, CRISC

Dan Hadaway founded Infotex in 2000 to help banks comply with the then-new Gramm Leach Bliley Act. Since then he has grown the firm to be a leading Managed Security Service Provider (MSSP) that also provides IT Audit services as well as IT Governance consulting. As one of the first to hold a CRISC designation, Dan helped write the review manual for the Certified in Risk and Information Systems Control certification (CRISC), which recognizes professionals for their knowledge of enterprise risk and their ability to design, implement, monitor and maintain information system controls to mitigate such risk. Dan speaks regularly at conferences and conventions, and facilitates an annual IT Security Conference for banks. His often humorous writings have been published in several publications as well as on his blog, my.infotex.com.