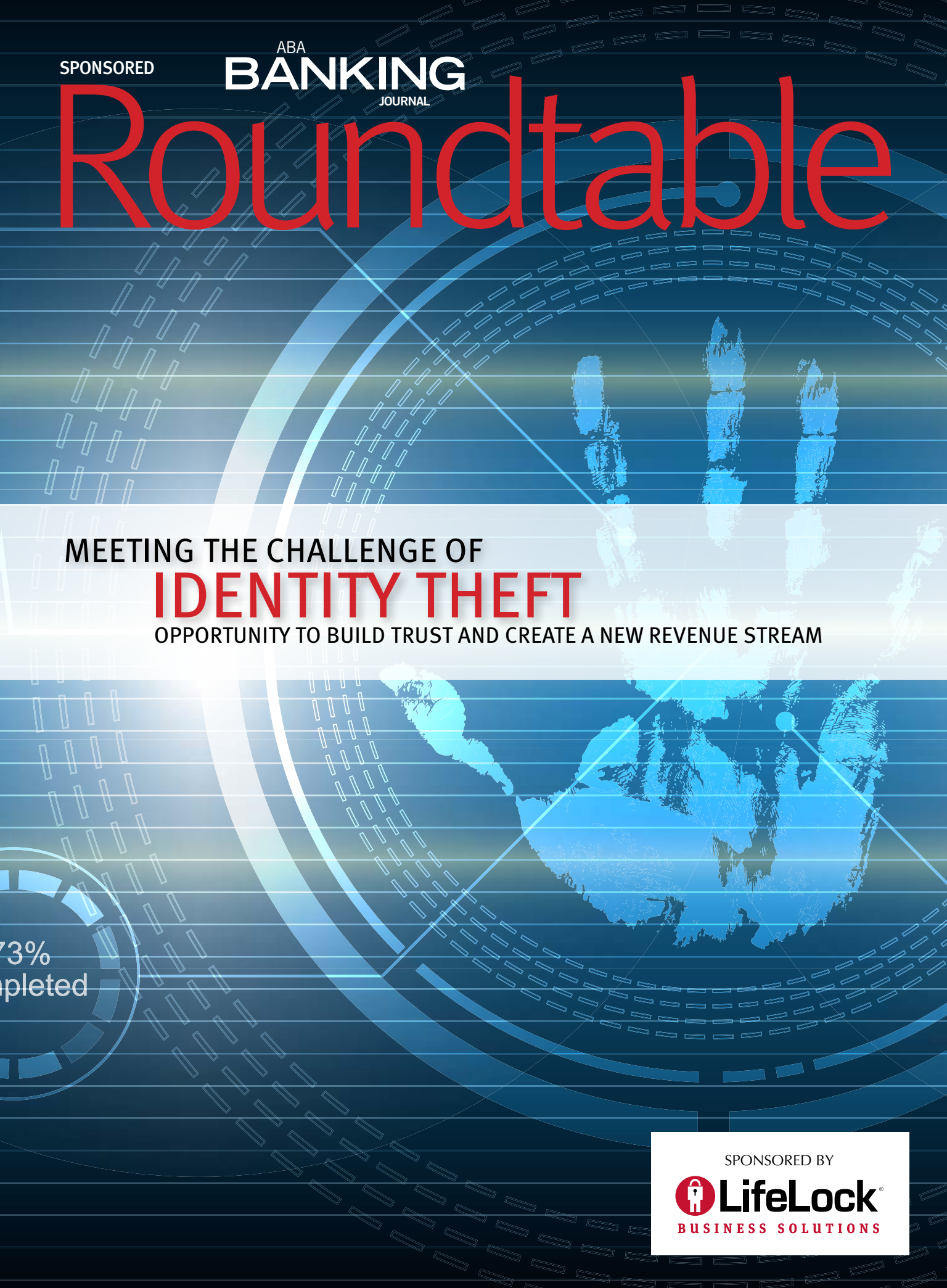
SPONSORED

ABA BANKING JOURNAL

Roundtable



MEETING THE CHALLENGE OF IDENTITY THEFT

OPPORTUNITY TO BUILD TRUST AND CREATE A NEW REVENUE STREAM

SPONSORED BY

LifeLock® BUSINESS SOLUTIONS

MEETING THE CHALLENGE OF IDENTITY THEFT

OPPORTUNITY TO BUILD TRUST AND CREATE A NEW REVENUE STREAM

Identity theft is a problem that is top of mind for many bankers and an obvious worry for customers. But is there more that banks can do to fight identity fraud? Panelists joined *ABA Banking Journal* and LifeLock Business Solutions at a roundtable to discuss trends in identity theft and banks' role in fighting fraud.

The banks gathered at the roundtable that offer identity theft protection have found it to be a natural offshoot of their current suite of products. Some of them are charging for the protection, while others are providing it to customers free of charge. All agree that identity theft protection is not only the right thing to do, but is also a way to deepen customer relationships.

Offering identity theft protection has regulatory and operational challenges, however. Panelists discussed how to comply with regulatory pronouncements surrounding outsourcing functions and services to third-party providers, as well as the type of due diligence that regulators require.

Perhaps most interesting were the conversations about how identity theft protection offered by banks can help restore the trust that customers have in the financial services industry. The good news is that with a bit of education, customers "get it." They understand that identity theft is rampant and that everyone is at risk. And with understanding comes appreciation that their bank is looking out for their best interests by offering products that can keep them from harm.

Here are brief introductions of the roundtable panelists:

Ted Awerkamp, chief operating officer, First Capital Bank of Texas, Amarillo, Tex. Fifteen year-old First Capital Bank of Texas is a $730 million institution.

Lucy Griffin, senior associate, Paragon Compliance Group, Washington, D.C. A compliance consultant for the past 20 years, Griffin also was a regulator and managed ABA's compliance division.

Jackie Silverstein, senior vice-president, director of bank operations, Savings Institute Bank & Trust, Willimantic, Conn. The $980 million bank recently became a $1.5 billion institution following an acquisition.

Eric Warbasse, senior director, Enter-

> *Account take-over attempts concern me most. Fraud evolves by the hour*

Kim Syrop

ALL INSIDE PHOTOS: ARNOLD ADLER

OUR ROUNDTABLE PANELISTS

Rick Arthur
Vice-President, Marketing Product Director
Union First Market Bank, Richmond, Va.

Kim Syrop
Senior Vice President, Fraud Mitigation and Loss Management
Webster Bank, N.A., Waterbury, Conn.

Ben Mendelsohn
Vice-President, Senior Retail Product Manager
Fifth Third Bank, Cincinnati, Ohio

Lucy Griffin
Senior Associate
Paragon Compliance Group, Washington, D.C.

Jackie Silverstein
Senior Vice-President, Director of Bank Operations
Savings Institute Bank & Trust, Willimantic, Conn.

Eric Warbasse
Senior Director, Enterprise Sales
LifeLock, Tempe, Ariz.

Ted Awerkamp
Chief Operating Officer
First Capital Bank of Texas, Amarillo, Tex.

William Streeter
Editor and Publisher
ABA Banking Journal, New York, N.Y.

prise Sales, LifeLock, Tempe, Ariz. Prior to joining LifeLock five years ago, Warbasse spent eight years in technology sales and marketing with Lenovo Group and Insight Enterprises.

Ben Mendelsohn, vice-president, senior retail product manager, Fifth Third Bank, Cincinnati, Ohio. Identity theft protection is one of the product lines that Mendelsohn oversees for the $126 billion bank.

Rick Arthur, vice-president, marketing product director, Union First Market Bank, Richmond, Va. One of the largest community banks in Virginia with $4 billion in assets, Union recently announced an acquisition of $3 billion Stellar One Bank.

Kim Syrop, senior vice-president, fraud mitigation and loss management, Webster Bank, N.A., Waterbury, Conn. Webster Bank provides a full range of commercial and retail banking services to customers from metro New York City to Boston, Mass. Founded in 1935 in Waterbury, Conn., Webster has grown to more than $20 billion in assets.

Panel moderator was *Bill Streeter, editor and publisher,* ABA Banking Journal, *New York.* Streeter became the magazine's editor-in-chief in 1987 and added the publisher role in 2012.

What follows is an edited report of the panel's lively discussion.

What identity theft activities are you most concerned about?

Kim Syrop, Webster Bank: There are several. Account takeover attempts concern me the most. Crooks are using malware, pretext calling, and other creative methods to try to gain access to customer accounts. New products, such as mobile banking and remote deposit capture, are inherently riskier than more traditional products.

Crooks are creative, and fraud evolves by the hour.

We also have seen more fraud attempts resulting from compromised credit reports. We can identify these because the customer account number on a credit report contains a unique bank prefix that doesn't appear on a customer's statement. If the caller provides the prefix as part of the account number, it may indicate it's an identity thief reading the account number off a compromised credit report.

> *We should feel really good that customers turn to their banker for advice when they're worried about identity theft*

Ben Mendelsohn

Ben Mendelsohn, Fifth Third Bank: It's great that the use of bill payment and mobile banking has exploded over the past couple of years. But on the flip side, customers are more comfortable giving out personal details online or over their mobile phones that criminals can use to social engineer their way to a customer's identity.

Eric Warbasse, LifeLock: Fraudsters often use a stolen identity to get a cell phone, so they now have a number with which to conduct further fraudulent activity. Banks need identity theft protection products that map into alternative databases and information sources.

Syrop: It's interesting that you bring up cell phones, because identity thieves will determine which consumers have good credit scores based upon the number of lines they're offered by a cell phone provider.

Mendelsohn: Did anyone change their voicemail or out-of-office messages to let people know they'd be out today? I ask because a thief will call someone in your office saying they know you are out and ask them to send something that contains your personal information. It's another way thieves use social engineering to access customer records and information.

Outlook has a feature you can turn on to send out-of-office responses only to internal contacts. The services are getting smarter, but social engineering is still scary.

Ted Awerkamp, First Capital Bank of Texas: One of my colleagues went to file his taxes, and, low and behold, he was told he had already filed them.

Warbasse: It's relatively easy to get the information needed to file a tax return through peer-to-peer file sharing. Say you're an accountant who brings home

tax return work, and your child uses these networks to share music. Thieves can access those tax returns stored on your hard drive. That's not really a banking problem, per se, but it shows how digitized data is readily accessible to criminal elements.

Do customers contact their bank, even if it's not a banking problem?

Mendelsohn: You know, they do. As an industry, we should really feel good that customers turn to their banker for advice when they are worried about identity theft.

Ted Awerkamp

> *If employees have access to ID theft protection, they see its value. If they don't understand a product, they won't sell it*

Lucy Griffin, Paragon Compliance Group: People turn to their bank for help, but they also are likely to blame the bank. Banks need to turn that perception around and deepen that trusted relationship.

Awerkamp: There is a bit of a disconnect. A lot of bad guys are trying really hard to steal customer identities, and customers can't expect their bank to analyze every check that comes through its systems.

Does it make sense for banks to offer identity theft protection?

Jackie Silverstein, Savings Institute: We are seeing customers reach out to us. But we have to balance our counsel with our reputation, since those customers may feel it's our fault they've given personal account information to a phishing site because they were using our online banking service at the time.

Rick Arthur, Union First Market Bank: We increasingly find ourselves in a counseling role when a customer is a victim of fraud, and we often guide them through the process of filing affidavits or police reports.

Arthur: Identity theft protection services are a natural extension of why customers come to banks. They have been bringing their deposits to us for years because we're FDIC insured. Now, we're extending that protection to their identity and their total finances—not just for their deposits.

Warbasse: We believe it does make sense. But when offering an identity theft protection product, you need to clearly explain to the customer what that product is protecting and what the bank is responsible for protecting.

Make it clear that the bank is doing everything in its power to protect customer assets and is now going above and beyond by offering customers an opportunity to protect their identity outside the bank.

Arthur: Right, and when they realize they can register the credit cards and debit cards they have at other institutions, they see that you are really expanding the protection you offer for their total financial picture—not just for what they have at your bank.

Griffin: Clarity and constant communication make a big difference in how customers would perceive identity theft protection. Identity theft protection changes over time. Newsletter updates or emails remind customers that they have responsibilities as well.

Warbasse: One benefit of proactive identity theft protection that banks can leverage is alert capabilities. When identity theft protection services are facilitated by the bank, and the member receives valid identity alerts as a function of those services, the bank may enjoy the benefit of a positive customer experience.

Compare identity theft protection to other bank products, such as life insurance, that customers sign up for and then forget about. Identity theft alerts are an opportunity to deepen the relationship with the customer since they don't want to forget about it; customers want to know that they're protected.

Do any of you currently offer identity theft protection?

Silverstein: We don't actively market identity theft protection to our customers, but we do offer it for free for several years in the unusual instance in which we've made an error that could compromise their identity. We don't use the product for income, but for loss mitigation and reputation preservation.

Mendelsohn: We've offered identity theft products since 2008—both proactively and reactively. It's a great customer engagement tool, and many customers feel that it's a core part of the reason that they bank with us.

Arthur: Three or four years ago, we started providing free identity theft resolution services with many of our consumer checking account products. Late this summer, we rolled out three new, fee-based identity theft protection packages. We'll need to educate customers on the added value offered by these new fraud and credit monitoring services, but for us, offering comprehensive identity theft protection services is a natural evolution.

Awerkamp: We did, at one time, [offer identity theft protection] as a value-added service to a club checking account, but it was limited to six months. The club—and therefore the service—has been discontinued.

Is there a particular customer demographic most interested in such a product?

Awerkamp: I imagine it appeals mostly to consumers over 40 years old, since they hold more assets than younger consumers. Is that true, Eric?

Warbasse: Demand does increase in proportion to consumer assets. But what's ironic is that the younger generation is at an increasing risk of identity theft, because they use social media and because many don't password-protect their smartphones.

Eric Warbasse

> *One benefit of proactive identity theft protection that banks can leverage is alert capabilities*

Mendelsohn: At Fifth Third, interest in the product really spans demographics. The fear of someone using your identity for something fraudulent is pretty universal.

Our experience is that customers with assets are worried about protecting those assets; customers without a lot of assets are worried about protecting their access to credit. It's counterintuitive, but protecting your credit history and identity is potentially even more valuable to someone who doesn't have a lot of assets than it is to someone who does. Someone with a lot of assets knows the bank already protects their assets.

Arthur: It seems like you need to connect the dots for those folks without a lot of assets, because they may not understand the need to protect their identity, credit, and good name.

Griffin: That's right. Young people are at risk. A friend of my daughter's applied for a banking job after graduating from college and discovered that she had a horrendous credit history even though she had never taken out any credit. Her student identity had been stolen.

Mendelsohn: Pick out those benefits that have the most impact to your broadest customer base, both young and older. Most customers are interested in identity theft protection. Unlike ATM withdrawals and online bill pay, this is a service that customers are willing to pay for.

Arthur: Even so, we will always have some customers who expect to get it for free. Part of the problem is that banks still offer many services for free—like free checking. An unintended result is that the frontline staff of banks and customers get conditioned to that and remain in the mindset that we must offer products and services for free.

How do you select an identity theft protection product?

Arthur: It comes down to balancing the value of the quality of the product

Regulators look more favorably on a bank that is proactive and nurtures a trusted relationship with its customers

to the customer and the value to the bank. Value to the bank from a particular product can be a lot of things. How turnkey is the product? What type of marketing support does the vendor provide? How much training support do you get? Also, the bank has to be sure that it's a partnership with fair revenue sharing.

But these criteria are table stakes, because banks have to get identity protection right or we're all going to take it on the chin. We're going to be talking to the regulators. And, like any new service, we're going to have some customer service issues. We're going to have reputation risk. I don't think there's a magic equation to figuring out that balance, but that's what's going through our heads when we're comparing vendor options.

Warbasse: When evaluating products, look at vendor support for operations, IT, marketing, and training. You need all four legs of the stool for the program to succeed. Although it's tricky to balance, we've found programs are most successful when bankers and tellers provide enough information to customers so they feel comfortable with the product without detailing how the product actually works. The onus for detailed information can't be on the bankers, so make sure the vendor offers resources for those customers who want more information.

Banks have to get identity protection right or we'll all take it on the chin—with customers and regulators

How do you train employees?

Silverstein: Staff training is pretty clear-cut. We regularly train our call center and IT staff. We obviously train the frontline folks and anyone who has contact with customers to ask the right questions. On the back end, we train anyone responsible for wire transfers.

Our challenge is customer training and figuring out how much information we should push out to them.

Awerkamp: We do not offer [identity theft service], but if we did, I would suggest if we offered it to them at a deep discount, they would understand the value such a service provides. They would receive the monthly reports and the text alerts and the training. If they don't understand a product, they're not going to sell it.

Syrop: We publish blogs and articles and have a "Fraud Fact" section on our external website. We train our frontline and call center staff on what to watch out for. We also do outreach to groups, such as senior centers.

Warbasse: A lot of banks host shredding events, and those are obvious opportunities to talk to customers about identity theft protection.

Mendelsohn: You can't expect your customers to become experts in fraud, but you can help them develop a filter and call their bank when they are unsure. You can educate them on how the information they make publicly available can be used for identity theft.

What does the ID theft protection revenue stream look like?

Warbasse: Every bank wants to monetize its customer base, but there are different ways to do that. It doesn't have to be through direct profits on an identity theft protection product. However if you can use that product to deepen the customer relationship and have a dialog with a customer whom you wouldn't otherwise have had that access to, then you can monetize them indirectly pretty effectively.

Mendelsohn: That's true. What we hear from customers is that they bank with us because of the value we provide. We're primarily offering identity theft protection to add value to the customer relationship. The fact that it generates revenue is nice, since there are a lot of things we do for customers that don't.

Early on, we created a free, preferred program for customers with more than $100,000 in assets with us. When we talk to those customers, it's not free ATMs or discounts on trades that they mention, but they really appreciate that we make identity protection a part of the relationship.

Syrop: In addition to revenue, identity theft protection has another benefit. A lot of account takeover fraud requires the thief to open a secondary account in a customer's name to move funds from bank A to bank B. We're responsible for those losses. In addition to customers feeling "warm and fuzzy" that they have this protection, we've benefited by minimizing losses.

Griffin: It's interesting because identity theft protection is not strictly a banking product, so it is truly extra.

Regulations require banks to respond when they receive a notice of identity theft, but identity theft protection takes it a step further in actively protecting and helping customers. It's an unwritten rule that regulators look more favorably on an institution that is proactive and nurtures a trusted relationship with its customers.

Is there increased scrutiny around using a third-party provider?

Silverstein: Vendor management is a big deal in terms of what we do on a day-to-day basis. We look not only at what technology the vendor is offering, but we consider what the entire vendor relationship will look like.

Syrop: I agree. Webster Bank is very focused on vendor management. It's serious stuff.

Griffin: Third-party due diligence is being pounded on by the regulatory agencies. The message is that when you outsource any kind of function, you are, in essence, outsourcing part of the bank. You must manage, monitor, and audit that outsourced function the same way you would if it were

Staff training on ID theft is clear-cut. Our challenge is how much information we should push to customers

conducted inside the bank. You have to either review the training or actually conduct the training.

Even if you outsource a service somehow connected with your bank, the regulators say that you are putting the bank's reputation at risk.

The challenge for vendors is that examiners are asking every bank to audit every vendor. How many times does a vendor want a bank dropping in to audit them? We have to come up with a better way to do this.

Silverstein: Vendor management falls under our risk-management umbrella, and we risk-rate our vendors on a regular basis. We know whether or not we're going to consider replacing one at the time of the contract or at the time that we review the vendor. When there's a lot of vendors to look at, it's easier to replace your vendor. But when there aren't a whole lot of vendors, the vendor you have may require a higher risk rating. The regulators want to know how closely you are paying attention to vendor risk and if you are writing risk-mitigation language into vendor contracts.

Warbasse: I know it may seem trite, but if you put the customer's interests in front of your own and you can represent that with confidence, the other stuff falls into place.

For example, a multi-step enrollment process can have breakage wherein a customer thinks he completed the enrollment process and is protected, but he hasn't completed the enrollment process because additional steps are required.

A single-step enrollment process may mean slightly lower acquisition rates, because of the requirement to ensure the enrollment was successful prior to charging the customer, but regulators look more favorably at sacrificing acquisition potential for a better customer experience. Would you agree, Lucy?

Griffin: You said it very well. It's abusive and deceptive practices that are problematic.

You have to repeat important information over and over since the customer may have only one ear open, but you're held liable for their inability to hear what you're telling them.

We've talked about reputation risk and trust. Have banks regained the trust lost due to the financial crisis?

Silverstein: That's a darn good question, but I don't know the answer because I can't really say how much the financial crisis damaged our reputation. As a community bank, a lot of our customers know us personally, so I think we're okay, but definitely the action of a few banks tarnished the reputations of all of us.

Mendelsohn: Customers still go to their bank for information, education, and when they have concerns. That speaks to the value of the personal relationship that customers have with their bankers.

But customers feel differently about their bank than they do about the overall banking industry. It's like they separate the two in their minds.

The real value of offering identity theft protection services is that it creates a halo effect. Customers want to bank with someone that will help protect them, and this product is evidence that we are doing just that.

> *Protecting your identity is potentially even more valuable to someone who doesn't have a lot of assets*
> **— Ben Mendelsohn**