WORKING TOGETHER TO PROTECT AGAINST

IDENTITY THEFT

BANKS SHOULD STRIVE FOR A PARTNERSHIP WITH THEIR CUSTOMERS
In 2012, 16.6 million people—or 7% of all U.S. residents ages 16 and older—were victims of identity theft, according to the Bureau of Justice Statistics (BJS). Of those victims, 7.5 million reported the fraudulent use of a bank account.

The majority of victims had no idea that their identity had been compromised until they were notified by their financial institution, notes BJS.

Financial institutions play a critical role in both protecting against, identifying, and helping their customers manage the aftermath of identity theft. At many banks, that role includes educating customers on the range of potential threats, including low-tech methods, such as dumpster diving, as well as high-tech methods, such as phishing, malware, and social engineering. Banks have long used their websites to disseminate information about identity theft and are now exploring additional avenues, including meeting with community groups and creating advisory councils.

Education doesn’t end with the consumer. Banks also are training frontline employees to speak to customers about ways they can work with the bank to protect against identity theft.

ABA Banking Journal and LifeLock Business Solutions invited a group of bankers to a roundtable to discuss identity theft trends and how financial institutions can educate and work with customers and employees to protect against identity theft. The bankers agreed that while they are working diligently with both customers and employees, there is more left to be done to help protect both customers and their institutions.

Here are brief introductions of the roundtable panelists:

Robert Franz, senior fraud risk manager, First Niagara Bank, Buffalo, N.Y. Franz has 28 years of banking experience. First Niagara has $38 billion in assets.

Dana Marsalisi, vice-president, anti-fraud officer, Valley National Bank, Wayne, N.J. Marsalisi, who has worked in fraud prevention for 18 years, is an 11-year veteran of the $16 billion financial institution.

Brian Higgins, first vice-president, product and e-banking director, First Niagara Bank.

There is a lack of accountability with identity theft. When a merchant has a data breach, the bank foots the bill, and, often, the criminal walks...
OUR ROUNDTABLE PANELISTS

Robert Franz
Senior Fraud Risk Manager
First Niagara Bank, Buffalo, N.Y.

Tammy Keffeler
Senior Vice-President
FirstBank Holding Company, Lakewood, Colo.

Eric Warbasse
Senior Director of Financial Services Strategy
LifeLock, Tempe, Ariz.

Kenneth Olan
CEO/Cofounder
CAKE Performance Solutions Houston, Tex.

Dana Marsalisi
Vice-President, Anti-Fraud Officer
Valley National Bank, Wayne, N.J.

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

Brian Higgins
First Vice-President, Product and e-Banking Director
First Financial Bank, Cincinnati, Ohio
What trends in identity theft are you seeing? Have they been impacted by the rash of data breaches this year?

Eric Warbasse, LifeLock: There’s a growing awareness among consumers about the risk that they’re facing. And correspondingly, the bankers that we speak with indicate that they’re more and more on the hook for answering questions about identity theft and having resources available. Right now, fraudulent credit card activity is all in the news. As chip-and-pin technology is deployed, it should reduce card-present fraud. But the concern is that card-not-present fraud will increase along with identity theft.

Dana Marsalisi, Valley National Bank: We’re seeing an increase in tech support scams. Fraudsters call customers purporting to be from Microsoft or Apple and claiming they found a virus on the customer’s computers. They then install malware on the computer to capture keystrokes and steal information.

Tammy Keffeler, FirstBank Holding Company: We’re seeing more identity theft from social engineering in which the customer provides personal information over the telephone because they think they are dealing with someone they can trust. The fraudster then calls the bank with the information they’ve gotten directly from the customer.

Marsalisi: And they are “spoofing” phone numbers, so the caller ID appears to be the customer’s phone number. The fraudsters have all the right answers and can answer the challenge questions, and even tell you when the last deposit was made.

Keffeler: We tell customers not to give out their account number, but they provide all types of personal information, such as their kids’ and pets’ names on Facebook. What they post online puts them at much more risk than their account number.

Marsalisi: What worries me about identity theft is the lack of accountability. For example, when a merchant has a data breach, the bank foots the bill, and it’s the reputation of the bank that’s on the line. Far too often, criminals walk away with a slap on the wrist.

Robert Franz, First Niagara Bank: I agree that accountability is a real problem. You can steal information very anonymously now. It’s difficult to track...
the criminals down and prosecute them.

**Are your banks concerned about identity theft targeting elderly customers?**

**Brian Higgins, First Financial Bank:** We continue to see alarming statistics showcasing how often older clients become victims of identity theft. A group of us at First Financial have been discussing ways we can help protect elderly clients and their families. Does anyone have any suggestions or current programs in place that have been successful?

**Marsalisi:** You have to train employees in the branches to identify elder abuse, and you really need to establish a good rapport with adult protective services in your area and help them understand that we must work together on this. Once you establish that rapport, they will jump on any issues you refer to them and will work together with law enforcement as needed.

**Franz:** I agree that a good relationship with adult protective services is key to identifying and mitigating elder abuse. Best practices like knowing your customer can also help identify issues early.

**What role does customer education play in helping reduce identity theft?**

**Keffeler:** A big role. We've already educated customers to tear up credit card offers they don't want before throwing them away. We now need to educate customers that when someone calls and starts asking for information, they need to consider whether the request is legitimate before providing personal information.

**Franz:** We have to educate customers that they are the first line of defense. They have to take steps to protect themselves.

**Marsalisi:** Many customers confuse credit card fraud with identity theft, so we're educating them on the differences. Their identity is not necessarily stolen if someone uses their credit card, but customers panic when they hear about data breaches that compromise credit card numbers.

**Kenneth Olan, CAKE Performance Solutions:** But if you steal somebody's credit card number, you now have a piece of information that you can use to get even more information. A lot of consumers don't understand the scope of what can happen.

**Franz:** We are using education to create a bank culture in which everyone is worried about protecting the bank, its customers, and its assets. What helps me rest a little bit easier is that I am seeing people becoming engaged, recognizing the problem, and then taking steps to ensure we have the resources we need to protect our customers and the bank.

**How are customers reacting?**

**Warbasse:** It's ironic. There's growing consumer awareness on the one hand, while on the other hand, there's increasing risk that consumers will become more apathetic. They won't be engaged with the bank if we don't give them a reason and an outlet to be engaged in helping protect their identities.

**Higgins:** Education is key. The more your clients understand identity theft and how it can impact their future, the more willing they are to listen and put recommended security measures in place. For example, if we provide...
clients with fraud protection, but don’t educate them on how to use it or how it will benefit them in the long run, they might find the service to be inconvenient or annoying.

But if you can change the way you communicate with clients about identity theft, you can change their mindset. We’ve taught our frontline associates to position security as a way for clients to achieve peace of mind. It’s not about getting the client to buy a product, but to understand why protecting themselves is so important. Our associates are excited about the opportunity to offer a service that will give clients more control and security.

**Warbasse:** Customers have an expectation that it’s the bank’s responsibility to protect them and, at the same time, provide an impeccable customer experience. To get customers involved in their own protection, we have to allow them to select the level of protection they want based on the risk they’re willing to take, and then reward them for taking steps that help reduce everybody’s risk. Rewards can take the form of incentives, eliminating certain fees or simply affirming that their efforts are appropriate, responsible, and appreciated.

**Higgins:** And give them some power to choose how they want to be communicated with about fraud. When you do, engagement levels increase dramatically.

**Olan:** If you want to get customers or employees more engaged, create an environment to engage them. For instance, establish a local customer advisory board or a banking center advisory council, and ask them what the bank should be doing about identity theft. Help customers see that the bank actually cares. If you can get customers involved in what you’re doing, and can get them feeling like they’re contributing to the end-game and aren’t just passive watchers, you can move mountains.

**Franz:** Frontline employees should understand why certain controls or procedures are in place. Associates can engage with customers and help them understand why those daily limits are in their best interest.

**Olan:** The biggest advocates for customers are on the front line. They’ve known Mrs. Jones for 25 years and don’t want to offer Mrs. Jones something that won’t genuinely help her with greater peace of mind, safety, and security. One of our best barometers of new products and services is how quickly the front line will adopt them.

**How should banks educate and work with customers?**

**Marsalisi:** Using your website to educate your customers is key. We have a fraud prevention checklist and an identity theft kit on our website and an identity theft help line. I also speak to community groups about identity theft and fraud.

**Franz:** You need to deliver that security message at every opportunity to build a community. That puts customers in a much better position to protect themselves and understand what tools the bank provides.

**Olan:** We become better organizations by collaborating with customers to help us create new products and services that get them involved. Once they feel involved, they feel a little bit more
empowered and that helps build a relationship with the bank.

**Higgins:** We also have a security page with access to information, videos, tips, and advice, but we’ve found it’s one of our least-visited web pages. We’re trying to be more proactive with alerts, and are having success with clients setting parameters for when and how we notify them. I think if we can work closely with each client and customize based on their needs and preferences, we will see better results.

**Warbasse:** There are two ways to help mitigate identity fraud risk. One is to try to lock down the data, but you can only go so far.

The second way is to protect against the use of the data. You can do that through encryption, but a more interesting way is to protect against its use by making the customer part of the process. If they get an alert that a transaction occurred that they didn’t authorize, the customer can contact the bank—or, in the case of an identity protection partnership, the provider of the service—helping ensure that stolen information cannot be fraudulently used.

Is anyone else sending alerts to customers?

**Keffeler:** We are. We allow customers to select from a menu of alerts from within our online banking system. Customers can choose to get an alert if their card is used outside the U.S. or if they have an ATM withdrawal more than a certain amount. We market this function heavily because customers feel more secure when they have a part to play and we love them being more engaged. Customers request all sorts of alerts. Having an in-house online banking system that we can customize with alerts is a huge advantage.

**Higgins:** We’re getting a lot of alert requests as well as requests for prepaid cards from customers who don’t want to use their credit or debit card online because they are concerned about e-commerce fraud.

**Warbasse:** Identity protection is probably the only retail product that enables a partnership between the fraud risk side and the retail side of the bank. Any time you get those two sides of the bank in sync with a common goal, you win.

And how do you get people to be on the same team?

**Higgins:** Engage all stakeholders early in the process, from ideation through deployment. Everyone has a legitimate part to play and can suggest ways to ensure that what we deliver to the client really provides value. Our fraud team understands where the industry is going. So they never put up roadblocks and prevent us from bringing a product or service to market. In fact, their perspective ensures that we do it the right way.

**Warbasse:** As a rule, if it’s in the best interest of the consumer, it’s going to be—by extension—in the best interest of the fraud team and the best interest of the retail team.
Franz: Exactly, but you have to combat the stereotype that the fraud folks will always say, “No,” by instead saying, “Let’s do it, but let’s do it safely.”

We’re lucky. Our online banking team recently began an initiative for another channel and invited our fraud team to their kick-off meeting. It was so refreshing to actually have that say right up front.

Keffeler: At our bank, both the retail and the risk sides of the bank want to work with each other because it does no good to sell something that loses the bank money or risks its reputation.

What do you do when your competitors offer a product that you view as risky?

Keffeler: We find ways to manage the risk, and if we can’t, we won’t offer the product. We then educate our frontline employees on why we chose not to offer it. But if our competitors are offering it, it’s pretty rare that we won’t be able to mitigate the risks to work for us.

Are you seeing more attention paid to providing identity theft protection to small business customers?

Warbasse: Banks are increasingly interested in offering small businesses a differentiated value by creating protection packages for small business owners if not the entire employee base.

Olan: At my previous bank, we were looking at how we could extend identity theft protection to the employees of those businesses. Our lenders loved that idea because it adds value to their relationship with their business customer.

Warbasse: If I have a commercial banking relationship with my bank and that relationship entitles my employees to additional benefits, it creates an association effect. Meaning the employees will associate access to the service with both their employer and the bank. We have a benefits distribution team focused on providing value through such arrangements.

Olan: There’s an employee productivity component as well. If an employee’s identity is stolen, they are distracted and not paying attention to their job.

What are some of the controls you have in place to reduce the risk of a breach?

Marsalisi: We have developed and implemented extensive internal controls focused on safeguarding customer information and sensitive data housed at the bank. And we constantly research new risks and educate employees on the best methods of preventing fraud. If you don’t have a robust and clear information security policy that people understand, you should. It’s not only a best practice, but is expected by the regulators.

Keffeler: When a customer logs in, we don’t rely on just the password, but also look at what computer are they logging in from and ask security challenge questions. We also don’t allow devices that can be plugged into the network. We have a trash audit so we don’t put sensitive information in the trash.

Franz: We also use security questions and a customer-selected picture, but it’s extremely important to make sure we’re
not making things harder for customers.

**Warbasse:** What I’m hearing again is this tension between protecting the data and communicating to customers what the bank is trying to accomplish. That’s why it’s so important that the marketing and retail folks share a common goal with respect to engaging consumers directly in helping reduce fraud risk. It may be as simple as having a pop-up bubble next to the password requirements at log-in that explains the direct correlation between password length and strength. By providing that information to the marketing department, the marketing department is equipped to engage the customer in a way that allows the customer to become part of the solution.

**Do customers actually appreciate the security measures banks take?**

**Keffeler:** I don’t see security as a marketing opportunity you can sell to customers. It’s just something you do because the alternative is so bad. It’s not okay for data to get out.

**Higgins:** Security should fit into your story. We feel that offering identity theft protection is a natural fit with our brand and our brand promise to our customers. If we truly want our help our clients, we must offer every tool available to help them meet their goals with the control, security, and access they desire.

**Franz:** Your information security audit should not be just an annual event. It should be ongoing, similar to customer education and awareness. It’s about changing culture and making employees and customers more aware and encouraging them to be proactive.

A digital world presents identity theft challenges, but I imagine it also provides challenges in differentiating your bank online.

**Olan:** It’s a question we often asked ourselves: How do we, as a regional bank, continue to add value in order to compete against the big banks? How can we differentiate our products and services so we can thrive in a way we can afford? We came up with several ideas. For example, we put business centers in six of our branches and created an affinity program, so customers could make copies or count coins, send faxes, and much more because we knew that a large bank with hundreds of branches can’t afford to do that.

**Keffeler:** One of our strengths is our fantastic branch network. But we do struggle with differentiating our service in an online world without the face-to-face interactions.

**Olan:** It is difficult, but initiatives like our business centers provided an opportunity to attract customers into the branch so we can engage with them face-to-face.

**Higgins:** To retain relevancy in a digital world, you have to continually change the definition of service. In the past, service was defined by greeting clients with a smile and asking about their family. Delivering exceptional service is the key to our brand, and it’s our goal to provide high-quality service every day in every client touch point.