WEBINAR TRANSCRIPT

FFIEC AUTHENTICATION GUIDANCE COMPLIANCE:

Detecting and Responding to Suspicious Activities

FEATURING

George Tubin, Banking/Security Analyst

Eli Katz, VP - Enterprise Strategies/Finance, 41st Parameter

Jodi Florence, VP - Marketing, IDology

Mike Byrnes, Director - Customer Authentication & Fraud Detection Solutions, Entrust

Transcript of the Webinar Panel Discussion

ISMG
INFORMATION SECURITY
MEDIA GROUP

FFIEC AUTHENTICATION GUIDANCE:

Detecting and Responding to Suspicious Activities

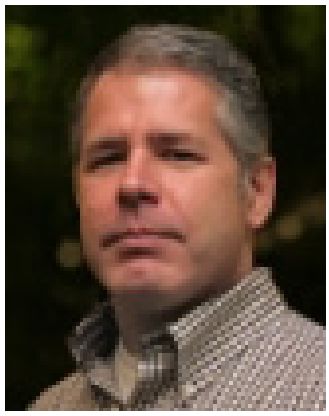
Sponsored by

This is an edited transcript of the roundtable discussion held in conjunction with the webinar *FFIEC Authentication Guidance: Detecting and Responding to Suspicious Activities*. Participants include Tom Field of *Information Security Media Group*, banking/security analyst George Tubin, Eli Katz of *41st Parameter*, Jodi Florence of *IDology*, and Mike Byrnes of *Entrust*.

GEORGE TUBIN
Banking/Security Analyst

ELI KATZ
VP, Enterprise Strategies/Finance,
41st Parameter

JODI FLORENCE
VP - Marketing,
IDology



MIKE BYRNES
Customer Authentication & Fraud Detection Solutions,
Entrust

See "FFIEC Authentication Guidance: Detecting and Responding to Suspicious Activities." VIEW WEBINAR NOW »

Since the summer of 2009, financial institutions and their corporate customers have been defrauded by increased incidents of account takeover. These incidents have pitted banks and customers against one another in court, and they were a key impetus behind the release of the new FFIEC Authentication Guidance. So, how can institutions improve their abilities to detect and respond to suspicious activities before fraud is committed? Read on to learn more from this panel of distinguished experts on:

- Today's most common fraud schemes preying upon institutions and their commercial customers;
- Strategies for improving early detection of account takeover attempts, as well as emerging methods of multifactor authentication;
- How to ensure conformance with this aspect of the FFIEC Authentication Guidance before your next examination.

The Panel

George Tubin,
Banking/Security Analyst
George Tubin is a former Senior Research Director for TowerGroup's Delivery Channels and Financial Information Security research services. His areas of expertise include consumer online banking, online fraud and identity theft prevention, information security strategy and customer authentication, as well as mobile banking and contact-center strategies and technologies.

Eli Katz,
VP - Enterprise Strategies/Finance, 41st Parameter
Eli Katz advises 41st Parameter's Financial Services clients on developing risk management strategies for protecting the Internet Estate. Katz joined 41st Parameter from Unisys, where he created and was director of the Active Risk Monitoring Practice. The practice specialized in creating risk-monitoring ecosystems that detect and analyze fraud or identity theft. In this role, Mr. Katz led the design of one of the first fraud systems to continuously monitor both online and branch activities.

Jodi Florence,
VP - Marketing, IDology
As Vice President of Marketing for identity verification provider, IDology, Inc., Jodi Florence's marketing experience spans 18 years. She has been actively involved in the identity industry for more than five years. Having earned a status of an expert contributor of fraud related articles to several ezines, Jodi is the main author of IDology's blog, IDentity Matters, where she focuses on top of mind identity issues including identity theft, fraud, data breaches, consumer privacy and more.

Mike Byrnes,
Director - Customer Authentication & Fraud Detection Solutions, Entrust
Byrnes has more than 20 years experience in technology product management, marketing and business development. He has been with Entrust for 4 years leading the company's Authentication, Fraud Detection and Secure Messaging solution areas. His responsibilities now involve leadership for Entrust's products and strategy for consumer and business banking, including solutions for strong authentication, mobile security and fraud detection.

Transcript

GEORGE TUBIN: What's the most important task for financial institutions between now and the timing of their next examination? Let me take a crack at that first.

I think the most important task is simply to get moving. Financial institutions right now are still doing a lot of thinking and listening to webinars, which is good, but they need to start some action. When the examiners come in, they're going to expect to see that the financial institutions have spent a considerable amount of time getting their programs implemented. If the program is not implemented completely, they really have to show that they've made a diligent effort to get this in place. It's something that should have been started back when the supplement first came out, not something that should be started in October or November. The institution really needs to be able to show the project plan and what they've been doing, and where they are now in the process. While I think every institution really does need to move toward full implementation, if they're not there they really need a well-documented project plan or good documentation of what they've been doing to get to where they are, and then have a very good explanation of when the full program will be implemented and in place so the examiner can come back and recheck at that point.

TUBIN: What are some of the vulnerabilities that are out there for out-of-wallet questions?

"When the examiners come in, they're going to expect to see that the financial institutions have spent a considerable amount of time getting their programs implemented."

GEORGE TUBIN

> "The biggest thing about when you talk about out-of-wallet questions or challenge questions in general is it's a lot easier for someone to guess your answers to your shared secrets."
>
> JODI FLORENCE

We'll go to Jodi for this one first.

JODI FLORENCE: That's a great question and definitely there are some vulnerabilities associated with where the question is coming from and how those questions are being generated. I think the level of risk about the data being compromised and people being able to easily guess your questions is a little bit far-fetched. In some cases, it depends on what kind of data you're using. Credit reports are definitely a lot easier to get a hold of these days, so when you're talking about public records data, you're talking about lots of different kinds of sources that are out there. For the fraudster to be able to go out and research all your public data records, you're getting a little bit more difficult.

The other issue is if you're using internal data, being able to prevent out-of-wallet questions based on your own internal data on your customers. This data is probably the hardest to be compromised because you're doing everything you can to protect this data, so that would be something that would help keep fraudsters from actually getting to your data. But I think the biggest thing about when you talk about out-of-wallet questions or challenge questions in general is it's a lot easier for someone to guess your answers to your shared secrets, which is why the FFIEC is making this move to replace these simple challenge questions with out-of-wallet questions. There's definitely a risk there, but it's not as high as some people believe.

Finally, I would like to see that the other vulnerabilities related to someone maybe guessing your question that isn't you or what have you, really point back to the tool that you're using. So, for example, you're using a solution that has lots of different features in place that are used to detect fraud, such as how many times has a certain question come forward, how many times has someone answered a question incorrectly, what kinds of questions are being abandoned, where are these questions being presented, etc. There are lots of different fraud features available within the tool that you end up selecting, and so you have to be very careful to make sure that whatever tool you do select does take into account that people can guess your questions and you want to minimize the number of red-herring questions and other things that indicate fraud.

TUBIN: That's great, Jodi. If I may add one more, and I would like to see if you would agree with me, I think another important consideration is the specific vendor for the out-of-wallet questions. All of these vendors will be supporting multiple clients to provide them out-of-wallet questions and the vendor really has to make sure they do a very good job of vetting out their client base to ensure that a fraudster isn't trying to sign up for their service, and then using that service to gather out-of-wallet questions for clients and trying to compromise.

FLORENCE: Absolutely, I would agree with that. On our side, we're a solution provider so we're not actually selecting the data and using that data. That's why we would urge people to use a solution from a solution provider as opposed to someone who's in the business of selling data, because they're more likely to have people that are on our client base that possibly are accessing the data just to get a hold of the data.

TUBIN: With so many new mobile devices hitting the market, how do you see the mobile fraud landscape evolving? That's a great question. Why don't we go to Mike for that one?

MIKE BYRNES: It's a very important question because more than ever we're seeing an increasing amount of smart phones in the marketplace, and I think sometime [in] late 2011, early 2012, there will be more smart phones shipped than regular phones, and there are good reasons for that. It's always on, it's quick-and-easy access to information and services, and it's intuitive. Unfortunately, with the growth of any type of financial vehicle or route to conduct a financial transaction, whether it's using checks or an ATM machine, or online banking, or e-commerce, when they grow in popularity it becomes a very attractive opportunity for criminals.

What we are starting to see in the marketplace is more and more what we would call mobile malware. For example, earlier this year there was a piece of malware called Gemini that targeted the Android devices and it was really collecting information, contact information, passwords, location-based information, and sending it off to remote servers for criminals to make use of in downstream fraud attacks. We've seen some rapid evolution. We're seeing a lot of phishing. Everyone is well aware of e-mail phishing attacks and attempts to get information, and we're seeing that on the

SMS channel, some people refer to that as "smishing." The attacks are now migrating toward leveraging the SMS channel. We're seeing man-in-the-mobile attacks trying to compromise the mobile device and compromise security mechanisms that use the mobile device. I just sense that as we move forward, and more and more applications and transactions are executed on mobile devices, the next major vulnerability area will be mobile browsers. You can deploy a mobile browser-based application or a native smart-phone application. I think mobile browsers would be attacked just like the browser has been attacked on the computer itself. It becomes a generic platform that a broad user base is using, so I think it may become a lot more vulnerable then say native smart-phone applications.

TUBIN: I think you make a great point. The fraudsters always go after the most vulnerable point, and institutions have been working with online banking and online web for a while, and based on this supplement they'll certainly boost their fraud prevention abilities, but the mobile area just hasn't been given the same amount of attention from the financial institutions, and even the mobile providers. The fraudsters will certainly go in and find the vulnerabilities and exploit them.

BYRNES: The other thing is, regardless of the security controls that a bank or a device has, at the end of the day a social-engineering attack, when a user is duped or tricked through a social engineering effort, you can't really protect against that. It's very difficult to protect against social-engineering attacks and we're seeing mobile users are being duped far more frequently then somebody say in a traditional e-mail or computer-based environment just because it's the nature of the mobile session; it's quick, quick access. You're in and you're out, so I think criminals will take advantage just of the usage of mobile with more and more social-engineering attacks, which will help them conduct their breaches.

TUBIN: That's a really good point. Let's take another question. You mentioned that more data is compromised than attacked. What does that mean and how should we respond to that? Let's go to Eli for this one.

ELI KATZ: Sure. There are a number of reasons why at any given time a significantly larger number of accounts will be compromised than actually attacked. On the consumer side, the number of accounts with high balances in them reflects the number of wealthy people in the population. So if a fraudster compromises accounts through phishing or through malware or any other means, they still have to go and weed through all these accounts to find the accounts with high balances. That of course leaves behind a wealth of footprints and information about what the fraudster's doing. Similarly, in the business banking side, even if a fraudster targets a certain company and compromises employees of that company, he still needs to figure out what employees have what rights and who's authorized to sign on transactions and so forth. That too requires a surveillance operation of going through the multiple accounts and looking at rights and so forth. And that has a number of ramifications.

"The next major vulnerability area will be mobile browsers."

MIKE BYRNES

One is that this is the fertile area to look to find fraud. Historically, we focused on transactional monitoring and if you wanted to find fraudulent transactions, look at the transaction. But looking at it from the perspective of account compromise, it makes more sense to focus on the fraud-staging events, both in terms of early warning and fixing things before the money actually leaves the bank, but also in terms of the sheer number of accounts that can be neutralized ahead of time.

The other implication, and it's a similar implication, link analysis, meaning using the information that you find in a single confirmed fraud to find other accounts that have been accessed by the same fraudster, is very useful and productive as well. We've seen cases where within a malware, through link analysis, we could find over 1,500 accounts or more linked to a single event and it could be online or even offline. It could be other online events or it could start the trigger of a fraudulent check where you go to the account and you see the preceding online staging event that preceded that event and you take it from there.

The last point is that, when you go through all these accounts, in addition to just looking at things from the account perspective, it's important to look at it from the fraudster's perspective, so not only anomalies that relate to the user behavior, but also patterns as it relates to the fraudster's behavior, and use it to derive intelligence that will be helpful in identifying that fraudster, in the future as well.

TUBIN: Great points Eli. I think you make a great point. Most institutions really think about stopping fraud as it's occurring, as the criminals try to move money, but there are a lot of indicators that the institution can use to sort of head them off at the pass and see when something is developing, and get in front of it before the actual fraud attempt is put in place. That's a great point.

We have another question. What are common challenges you're seeing as institutions prepare to conform to the FFIEC guidance? I'll take that one first.

I think that there are actually a number of challenges. One of the big challenges is that most institutions are sort of sitting, waiting and watching to see what other institutions are doing to conform with the FFIEC guidance. It's sort of similar to what happened the first go around back in 2005. A lot of institutions watched what some of the big banks, like Bank of America, were going to do. Once they saw what was put in place, they sort of followed, thinking that this will get [them] to comply. But I don't think financial institutions can really afford to sit back, wait and take that amount of time. I think that institutions really do have to get going and get moving, as I mentioned before. I think a lot of institutions are having a hard time with connecting fraud-prevention techniques and technologies with the identified risks that they have within risk assessments, being able to coordinate the technologies in a seamless and effective way, to make sure that the layered security program works and actually is coordinated and they get the maximum effect from it, while at the same time minimally affecting their customers.

I think the bottom line is to really get going with the risk assessment and really start matching up fraud solutions to the identified risk and reaching out to vendors and using the vendors' knowledge that have been in the space for a while to help you put the appropriate program in place.

BYRNES: I think I'd add to that, George. As a bank or a financial institution looks at the technology options that are out there, trying to discern what the best option is or what are the best approaches to build their layered approach, who are the best vendors that I should look at, it can be an overwhelming task and certainly it's an ongoing task. To help that out, I would recommend, when you consider vendors or reach out to them, ask them to provide input to help you put together the documents you're going to use to really size out which vendor is right for you. Don't try to do it all alone, but leverage the vendors for knowledge and key questions that should be asked of all vendors, that way you can hopefully get a good cross-section to more effectively pick the solutions that are right for you.

TUBIN: That's a great point Mike. … There are certainly a handful of vendors out there that are claiming that the use of their technology allows the financial institution to comply with the requirements and the supplements, sort of intimating that all they have to do is implement what this vendor has and they'll be all set in terms of compliance, when certainly there's not

“More and more banks are now starting to leverage native smart phone capabilities.”

MIKE BYRNES

one vendor that could come in and fully help an institution comply with the entire supplement. They're really going to need to work with multiple vendors and sort of also put together other pieces of the program like customer education and so forth. It's just not something that an institution could reach out to one single vendor to help with.

FLORENCE: I would like to add something to that too, because you bring up a very good point, and we're seeing that financial institutions are taking this project of FFIEC as a whole instead of bringing it down into its components and trying to figure out where are the biggest risks and where should I get started. Sometimes it's as easy as getting started with one vendor or getting in place a process in one area and then moving on to the next step. It doesn't all have to be accomplished at once. Mapping out a strategy to get from point A to point Z, there are lots of different steps you can take and you're not certainly going to jump from A to Z overnight.

TUBIN: Here's another question regarding out-of-wallet. How hard is it to get customers to transform from simple challenge questions to out-of-wallet, and how do you change their behavior?

FLORENCE: If we're talking about banks as customers, that's a lot more difficult to do, but I think we're probably talking about consumers of customers. The beauty of our questions vs. simple challenge questions, which we refer to as shared secrets, is there's no change. You don't have to do anything with your customers. It's just a matter of displacing the shared secrets with an out-of-wallet question. We've had this dynamic and it doesn't involve a consumer picking out the answers or picking out the questions and providing the answers to begin with. You can start using it the minute that you basically implement it. It's a very seamless switch.

I think what's important here though, and what you're probably really asking, is how well customers are going to embrace this.

The fact is that consumers don't really like the shared secret. They forget their answers. They forget their questions. It's capitalization issues. It's "what was my favorite food the day that I created the question?" There are lots of different reasons why consumers don't like the shared secret. We find that people actually really like the out-of-wallet question because they don't have to do much, and if the person is who they say they are, they can usually very easily answer these questions. Certainly they may forget something if it's based on their way distant past, but for the most part these are all types of top-of-mind questions that you can answer very easily.

But another issue of banks is getting them as customers to change. It goes back to what I was saying in the previous question, that you have to look at it and see where the biggest risk is and where you can basically make a change pretty quickly. Online, it's a simple API call to use an out-of-wallet question. So API XML calls back and forth and integration is pretty seamless and easy. In fact, at IDology we've had one customer, a very large financial

> "We've seen cases where within a malware, through link analysis, we could find over 1,500 accounts or more linked to a single event."
>
> ELI KATZ

customer, who implemented over a week and then was running transactions on Monday. It's not a difficult process. We find that it's more of an internal struggle to figure out the business processes as opposed to the actual technology.

TUBIN: Looking at it from a consumer perspective, when I've actually demoed some of these out-of-wallet questions, I thought it was really cool. I was in there and I was looking at some of the questions that were being asked of me. It was almost like "life trivia," going back and looking at really interesting things, and I actually wanted more and more questions to keep coming up just to see what they come up with. I found it to be very interesting.

FLORENCE: It definitely is and it can take you down memory lane, that's for sure.

TUBIN: Here's another question. What are some of the best practices you see among financial institutions using mobile as part of a layered-security program? Why don't we go back to Mike for that one?

BYRNES: I would start by saying that over the past few years, several financial institutions have rolled out SMS-based notifications to their customers, advising them about account activity. For example, if the user conducted a money transfer after the transaction, they would receive notification that money was transferred, this amount, or maybe they paid a bill or they purchased a certain item. It's this post-transaction notification. It could also be if a user changed their contact information, maybe their e-mail address or the phone number of their account, the bank would send a confirming e-mail or more commonly, since we're talking about mobile, an SMS notification. It's great because they're leveraging the user's existing device. It's fairly easy.

One of the downsides is it's not real time. It's after the transaction has occurred, after potentially a criminal has obtained money. Banks have evolved from that. They started using mobile devices to actually either send a one-time passcode to that device or generate a one-time pass code on a mobile device for strong authentication for online banking, and now where we've really seen the power of mobile being harnessed is with out-of-band transaction verification, where transactions or details are sent to the user in real time, prior to that transaction being completed, to essentially defeat a man-in-the-browser attack, to make sure that the transaction details are correct and they're confirmed through a separate, independent channel. We've seen that using SMS.

As we've talked about, we've seen some challenges with SMS, with man-in-the-mobile Trojans. But more and more banks are now starting to leverage native smart-phone capabilities. Most banks out there now have a mobile-banking application of some fashion, and if they can integrate technology such as out-of-band transaction verification into their own mobile banking application, they aren't only rolling out security in a simple to use integrated fashion, but they're really providing some cool features that are fighting security, features that are simple to use and really help their own brand and bank appear to be progressive and advanced in a customer-friendly type of way.

TUBIN: Thanks. There were definitely some critical points you made there, that institutions really do have to make sure that this is as simple to use as possible and integrating it into their online or mobile banking capabilities as a way to do that. I think the other point you made around including transaction information is just absolutely critical. The use of simple, one-time passwords sent to the mobile device via SMS just doesn't cut it anymore. As Mike said, we've seen malware, man-in-the-browser type malware, [which] gets around. Most of the fraud prevention capabilities that are in place right now, by simply sending a one-time password, the client really has no idea what it is that they're actually authorizing. It's really now at the point where it's critically important to include the transaction information so that the individual knows exactly what it is that they are authorizing.

We have one more question here. With so many customers now using multiple devices, particularly when we look at mobile, how should this change our approach to device identification? Let me go back to Eli for that one.

KATZ: That's a great question. If you look at the household today, and the coming years, it will have quite a bit of devices associated with it. So a husband and a wife, each of them would have a work computer, a home computer, maybe an iPad. The kids would probably have smart phones; they would have one or more gaming consoles. There may even be Internet access on the refrigerator door, and I'm not just throwing that out there because we actually saw a case of fraud emanating from a refrigerator door, believe it or not. When you look at so many devices per household, it raises a couple of issues, some trivial and some more interesting. At the trivial level, we need to check that our systems can handle, in terms of remembering and associating devices with accounts, large numbers of devices per household. Since all of us would have thought it ludicrous that households would have more than ten devices in them, chances are the system developers took the same stance say five, six, or ten years ago. It's worth checking to see whether your systems can handle and remember all these devices.

But at the more significant level, we've been talking in the past of creating customer profiles and checking for anomalies and what would constitute an anomaly of fraudulent risk, a fraud risk against the user profile. Maybe it's time to start thinking about associating roles with devices within the household. Yes, that household may make mortgage payments or send wires, and yes that household may make $5 PPP payments, but it's very possible that it's not coming from the same device, and being able to say, "Here's a transaction that may be normal for this household with a very typical device," may give us another layer of intelligence and another way of looking at the issue.

TUBIN: Very interesting as well. All these devices that are helping consumers simplify their lives create more complex problems for financial institutions when it comes to evaluating potential fraud.

> "The fact is that consumers don't really like the shared secret. They forget their answers. They forget their questions"
>
> JODI FLORENCE

KATZ: That's true.

TUBIN: I think that's all the time we have now for questions. Let me turn it back over to Tom now.

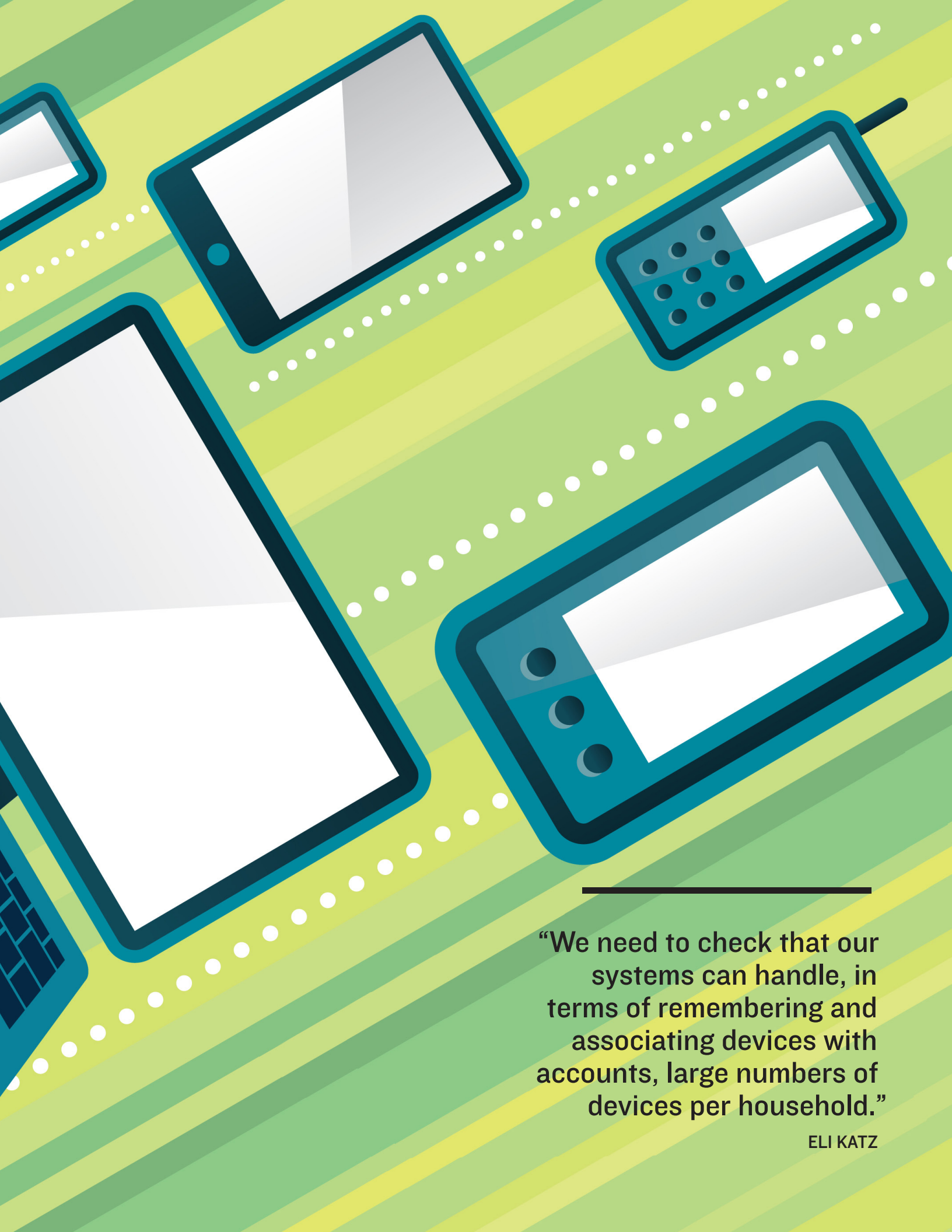
FIELD: Very good George. Thanks very much. I've got a couple of questions that I want to throw out for myself. One, George, is for you. Based on everything you've seen in the marketplace, and what you know of the federal regulators, when it comes to detecting and responding to suspicious activities, what do you expect the examiners really are going to hope to see when they conduct these first examinations in 2012?

TUBIN: I think the bottom line of what they're really looking for is for the institution to understand the threats, hopefully with a very comprehensive risk assessment, and laying out what the threats are, then being able to tie very clearly fraud-prevention capabilities that they have in place to each of the threats and demonstrate how the threats will be mitigated by using those technologies. That's important to actually show that the technologies work as they say they do.

For example, back in the first go around when a lot of institutions used secure cookies, the examiners ultimately found that a lot of banks implemented cookies that weren't very secure, cookies that could easily be copied to another device, and that's certainly not the definition of a secure cookie, although the banks claim that's what they had. The regulators or examiners are going to look a little bit deeper this time, and not necessarily just take each institution at their word, but really dig in and get a better understanding of the particular technology they're putting in place. I think they'll have a much deeper understanding of each of the vendors that are out there in the space and what the technology is that they provide so they could do a much better assessment of how well the technology actually works at practice.

FIELD: That's good insight. There's just one question I would like to ask of each of you briefly. We've talked about so much today. We've talked about certainly the FFIEC guidance. We've talked about out-of-wallet questions, mobile as part of a layered security program. We've talked about device identification. I'd like to ask each of you, and Jodi I would like to start with you, if there is one single point you would like people to take away from everything we've discussed today, what would that point be?

FLORENCE: … The biggest point I'd like people to take away is something that George said, and that's that the institutions really do need to get moving, because when we've been talking with people there seems to still be this "wait and see" mode as to what it all means, especially as it relates to out-of-wallet questions and challenge questions. I think the sooner that you make plans and get out of the "wait and see" mode, the better off you're going to be come January and later into 2012.



"We need to check that our systems can handle, in terms of remembering and associating devices with accounts, large numbers of devices per household."

ELI KATZ

FIELD: Excellent. And Mike, the same question for you. If there's a single point you would like the audience to take away, what would that be?

BYRNES: Speaking to a lot of different people from financial institutions at various events, conferences, etc., one of the big challenges that they face is that they often have been painted into a corner with a particular type of solution that at the time solved the given problem, but as the landscape moved on, as criminals became more sophisticated, that particular point product was no longer effective and no longer useful, and didn't allow the financial institution to keep up with the criminals. When you're looking to put in security controls for whatever mechanisms, whether it's the authentication piece or the fraud detection piece, look at a platform as opposed to a point product, something that allows you to meet the device user needs in front of you, the device channels you're trying to protect, and something that has been proven to evolve over time as criminal threats evolve and as customer needs evolve, whether it's simplicity or level of security or what have you. I would recommend looking toward a technology platform that really provides that evergreen-type of capability and will allow them to continue to grow without having to change out technologies every 18 months.

FIELD: Very good advice. Eli, the same question I would pose to you. If there's one thing you would like the audience to take away from our presentation today, what would that be?

KATZ: I would say start with intelligence and visibility, not only the spirit of the FFIEC guidelines, to understand what your risks are, but also as the industry moves toward offering more products online and through mobile devices, risk management becomes a product enabler and a revenue generator, and having intelligence and having visibility will allow you to have a fact-based strategy.

FIELD: Very good. George, I will give you the last words here. What are your final takeaways for the audience?

> "Institutions really do have to become better educated about what's happening out in the online world, or the electronic world, and make sure that they're constantly monitoring and ensuring that they have the right programs and policies in place."
>
> GEORGE TUBIN

TUBIN: I agree with everything that's been said and I think the regulators put out this supplement because they really needed to raise the bar in the industry. While some of the leading institutions really are doing a great job when it comes to understanding threats and putting in appropriate fraud detection and prevention technologies and programs, the vast majority of financial institutions just aren't as aware of the threat landscape and what's there now and what's coming down the road. The regulators want them to have a better insight into that, as we see more and more transactions shifting to the electronic channels. Online and certainly mobile transactions are increasing at a phenomenal rate.

Institutions really do have to become better educated about what's happening out in the online world, or the electronic world, and make sure that they're constantly monitoring and ensuring that they have the right programs and policies in place, not just waiting until the regulators force the institutions to do something. And the institutions, rather than viewing this exercise as a "what do I need to do to comply" exercise, really primarily look at it as "what do I need to put in place to best defend my customers and my organization against fraud?" I think if the institutions take that view, they'll comply with the guidance; and of course they'll need to go through the guidance supplement for all the nuances that are in place. But the real perspective has to be, "What do I need to put in place to best defend my institution and customers?"

VIEW WEBINAR NOW »

Don't miss "FFIEC Authentication Guidance: Detecting and Responding to Suspicious Activities"

http://bit.ly/vhub6I

About ISMG

Headquartered in Princeton, New Jersey, Information Security Media Group, Corp. (ISMG) is a media company focusing on Information Technology Risk Management for vertical industries. The company provides news, training, education and other related content for risk management professionals in their respective industries.

This information is used by ISMG's subscribers in a variety of ways—researching for a specific information security compliance issue, learning from their peers in the industry, gaining insights into compliance related regulatory guidance and simply keeping up with the Information Technology Risk Management landscape.

Contact

(800) 944-0401
sales@ismgcorp.com

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY® CAREERS INFO SECURITY® Data Breach Prevention. Response. Notification. TODAY

ISMG INFORMATION SECURITY MEDIA GROUP

4 Independence Way • Princeton, NJ • 08540 • www.ismgcorp.com