Good morning!

I am thrilled to welcome you to the ABA/ABA Financial Crimes Enforcement Conference.

This event has been going strong for 35 years, and we are so grateful for our partnership with our co-hosts at the American Bar Association.

Whether you’re joining us in person here in Washington, or watching virtually, thank you for spending your time with us during this busy holiday season.

I’d also like to extend a special welcome to the many government officials who are joining us from the federal agencies and law enforcement divisions.

You are critical partners to bankers in the fight against fraud and financial crime. And that fight has never been more complex and challenging than it is right now.

REFLECTION ON THREAT LANDSCAPE

I spent the early days of my career in financial services at the Treasury Department, working in the George W. Bush administration when 9/11 happened.

That event was a watershed moment for our nation—and one that changed the threat landscape forever, as well as how we approached financial crimes.
In the days that followed, the financial industry was enlisted to join the fight in the war against terror.

And that work continues today... at a time when the threats are more dangerous, and the stakes are higher than ever before.

Just look at recent examples from the news: the U.S. subsidiary of ICBC, China’s biggest bank, was hit by a cyberattack—right as Treasury Secretary Janet Yellen was meeting with her Chinese counterparts.

In this case, financial firms and the relevant federal agencies moved quickly to limit the damage and protect the system.

Just last week, we saw the Justice Department impose a $4.3 billion criminal penalty on Binance - the world’s largest cryptocurrency exchange - for failing to comply with the Bank Secrecy Act and other rules designed to protect the financial system.

Binance’s CEO pleaded guilty to money laundering and forced to step down. That followed the government’s successful prosecution of FTX’s Sam Bankman-Fried for fraud, which only highlights some of the new risks in play.

As the threat environment has evolved, we’ve also seen the financial crimes practice evolve and expand, with the convergence of the AML/CFT, sanctions, fraud, and other disciplines inside the bank.

The work you do at your institutions has major local, national, and global implications.

Your vigilance helps keep people safe, not just here at home, but around the world.
And as the only trade association representing banks of all shapes and sizes, I want to emphasize that ABA is here to support you.

So this morning, I’ll share with you several key things ABA is doing to bolster you and your banks as you fight on the front lines against financial crime.

**FRAUD**

Let’s start close to home, with the fight against fraud.

Over the past few years, we have seen what can only be characterized as an explosion of fraud activity—particularly check fraud.

It’s something I consistently hear from bankers across the nation:

Check fraud is a serious problem, and one that has affected hundreds of thousands of bank customers in the last year alone.

At ABA, we started asking ourselves what else we could do to support banks in tackling this pervasive issue.

Are there ways we could help banks improve fraud resolution processes? Are there efficiencies we could help create?

In talking with bankers, we learned that one of the pain points was the time it takes to process check fraud warranty breach claims with another institution.

Those conversations led to the development of ABA’s Check Fraud Claims Directory, which we launched earlier this year.
Our goal was to provide a one-stop resource for banks to be able to access the information they need to file a check warranty breach claim with another bank.

If your bank isn’t already participating, I urge you to sign up as soon as you can.

We’ve received overwhelmingly positive feedback on this initiative, and to date, we have more than fifteen hundred institutions that have provided information to the database.

You can visit aba-dot-com-slash-CheckFraudDirectory to learn more.

It’s open to all banks, as long as you’re willing to provide your institution’s contact information.

I can also share that we are working collaboratively with the U.S. Postal Inspection Service to address the significant amount of fraud being perpetrated through the U.S. mail.

By working together, we see opportunities to educate the public on how to safely use the mail system to pay your bills, while also taking advantage of the other payment platforms banks offer.

We’ll share more details on our collaboration in the coming days, but in the meantime, I hope you take the time to attend ABA’s Jim Hitchcock concurrent session on this topic later this afternoon.

ABA is also working to help banks educate their customers about the risks and red flags associated with common types of fraud and scams.

I hope by now, all of you are familiar with our award-winning #BanksNeverAskThat anti-phishing campaign.
We are thrilled that this campaign is back for its fourth year, with a host of new resources in both English and Spanish.

Banks can register for free to take advantage of the many resources we have to offer, just visit aba-dot-com-slash-BanksNeverAskThat.

We’ve had more than twenty-two hundred banks participate in the campaign. I urge all of you to make sure your bank is part of this important industry effort to educate consumers and stick it to the scammers. You can sign up at aba.com-slash-BanksNeverAskThat

AML/CFT/SANCTIONS

Now let’s zoom out for a moment and talk about the global picture.

We have two wars currently underway, one in eastern Europe, and now one in the Middle East.

We have state actors in places like Russia, China, North Korea and Iran escalating their use of cyber warfare.

And of course, we have ongoing issues related to the financing of terrorism, human trafficking, drug trafficking, and more.

Given the massive scale and global reach of these threats, it’s impossible for one bank... or one law enforcement agency to fight back successfully alone.

Collaboration is required.

One of the most important tools we have to combat financial crimes is shared information.
Banks collect a lot of good information on their own—but sometimes another institution might hold a critical piece to the puzzle that can really make a difference.

But in order to get the full picture, there have to be opportunities for information to be exchanged.

Banks have the ability to share information between themselves related to money laundering or terrorist activities under Section 314(b) of the USA Patriot Act.

But we understand from our members that there are some challenges in trying to access that information in real-time and connect the dots.

Processes can be inconsistent across different institutions.

Information sharing efforts can often prove ineffective, due to a lack of actionable information being shared in a timely manner—or even at all.

That’s why ABA has been focused over the last two years on working with our members to develop a framework for an information exchange that focuses on fraud, money laundering and terrorist financing risk.

We formed a consortium of around 20 banks to design and develop a new information sharing exchange—which ABA will manage.

The goal here is to leverage the 314(b) safe harbor among the banks involved in the consortium to encourage the sharing of information in real-time that can then be used to defend against fraud and money laundering.
We’ll be testing this application with our pilot group of banks in early 2024, with the long-term goal of being able to offer this service to any financial institution covered under Section 314(b) at a later date.

We believe this effort can make a real difference in fighting financial crime.

You can learn more about this ABA initiative at one of two sessions we’re offering tomorrow afternoon.

**IMPORTANCE OF EDUCATION**

Information really is power—and that’s one of the reasons we hold this conference each year: to provide you with the most up-to-date, expert information on fraud, financial crimes, BSA compliance, AML/CFT and so much more.

It's also why ABA has beefed up its other educational offerings in the financial crime disciplines.

In addition to this conference, we also launched the Certified AML and Fraud Professional certification program a few years ago, to train the next generation of financial crimes specialists.

We know that criminals never stop learning new ways to defraud customers and evade the law. And bankers can’t afford to stop learning, either.

To that end, and to complement our existing educational offerings, I am excited to announce today that ABA is launching a new AML and Fraud School in 2024.

This virtual school will be led by industry experts who will provide AML and fraud professionals with the skills they need to support a strong financial crimes enforcement program within their banks.
We need to stay a step ahead of the bad guys, and this school will help us do that.

Be sure to drop by the ABA booth in the Hub to learn more.

**IMPORTANCE OF COMPLIANCE PROS**

Beyond the areas of focus I just touched on, ABA is hard at work on many other challenges in the financial crimes space.

We’ve been incredibly active in the implementation of the various provisions of the Anti-Money Laundering Act, including the Corporate Transparency Act, which we championed in Congress.

In just five weeks, FinCEN’s beneficial ownership reporting rule will go into effect.

This is a major expansion of FinCEN’s mission.

We’ve been providing feedback—loudly and often—to FinCEN as the agency works to successfully implement this important initiative, which creates new reporting obligations affecting over 32 million small businesses.

We continue to encourage FinCEN to publicize and communicate new reporting requirements to the business community.

And we continue to push for greater clarity in the BSA/AML compliance rulebook.

For example, we’re pushing Congress to finally pass the SAFER Banking Act, which would allow banks to offer their services to cannabis businesses in the 39 states that have legalized cannabis in some form.
It doesn’t make sense to have these cash-intensive businesses outside the banking system. It’s a threat to public safety and transparency, and Congress has a great opportunity to do the right thing and fix this problem.

I’ll have plenty of time to go into greater detail on some of these initiatives in our next session, but as I close, I want to emphasize to this audience that the work you do really matters.

CLOSE
And I’d like to share a story that drives home the tremendous impact banks like yours can have:

This story comes from a $1.3 billion community bank in Southern California, where cryptocurrency investment scams—so called “pig butchering” scams—have risen significantly.

A customer came into the bank—a 32-year-old female, a student—to open a new account.

Not long after, this individual received a THREE-HUNDRED AND FIFTY THOUSAND DOLLAR tax refund check from the IRS. She then tried to make several subsequent withdrawals and wire transfers.

The bank’s BSA team was concerned, but didn’t have enough to act on.

...And even law enforcement didn’t have enough information to see the whole picture.

However, they were able to make a request to another local bank under Section 314(b), where the customer had also opened different types of accounts.

When they put all the information together, they had enough to show law enforcement.
They also got the IRS and the Secret Service involved, and what they discovered was that this customer had been groomed for over two years by an individual purporting to have a crypto investment business.

This scammer had successfully filed a fraudulent tax return in the victim’s name, and was having her withdraw those funds and feed cash into a crypto ATM... sending it back to the person she thought she was having a romantic relationship with.

Thanks to the hard work and due diligence of the bank’s BSA team, they were able to stop those funds from leaving the bank—saving the U.S. Treasury from a loss of over a quarter of a million dollars, and saving the victim from further harm.

They were also able to provide law enforcement with the contact information of the scammer, who is believed to be part of a much larger operation.

Law enforcement is currently following up on those leads—potentially stopping countless other people from becoming victims.

Bankers in this room know that this story isn’t unique.

At every bank, on a daily basis, financial crimes professionals like you are working hard to protect your customer from scams like this one.

It’s tireless work, and often underappreciated, because you can’t always talk about your successes. Sometimes you don’t even know what happened to the Suspicious Activity Report you filed.
And while you may not always receive the recognition you deserve from your clients, from your communities, or even from people within your own bank—please know that I see the Herculean efforts that you make to keep our financial system safe and sound.

And as I bring my remarks to a close, know that I do so with the utmost gratitude and admiration for each and every one of you.

THANK YOU.