Nasdaq VERAFIN
A STEP AHEAD

2024

Global Financial Crime Report

Insights at the Intersection of Financial Crime Data & Real Survivor Stories

Message from Nasdaq's Chair & CEO

Financial crime is a multi-trillion-dollar epidemic that underpins many of society's most insidious crimes from human trafficking to elder abuse to terrorism — crimes that exploit the most vulnerable in our society with activities that threaten the very integrity of our financial system.

Financial institutions have been at the forefront of this issue for decades and continue to be actively engaged and invested in this fight: our survey of anti-financial crime professionals found that 75% of respondents reported an increased investment in headcount in 2023 compared to the previous year. Financial institutions are responding to the intense pressure to effectively prevent fraud, uncover money laundering, and ultimately safeguard the financial system — all while ensuring they fulfill regulatory expectations despite facing inefficient processes, rapidly-evolving technology, and ever-increasing operational costs. Today, they are working to incorporate cutting-edge techniques and technology, including artificial intelligence to improve the efficiency of their processes and better detect threats.

Despite the enormity of the problem, historically it has been difficult to quantify the scale of financial crime with precision, given how much crime goes unreported by victims and undetected in today's financial system. Nasdaq's *2024 Global Financial Crime Report* is a new research initiative that aims to bolster efforts to root out criminal activity by supporting industry, policy and regulatory bodies, and other organizations with data and insights to help quantify the problem, elevate emerging threats, and uncover solutions towards a more integrated and holistic approach in the fight against financial crime. By bringing together expert research and data, industry perspectives, and the voices of survivors, this global report provides a unique view into the scope and impact of financial crime — and the scale of coordination needed to address it.

The report findings point to an incontrovertible truth — that the scale and pervasiveness of financial crime is immense. In 2023, more than three trillion dollars in illicit funds flowed through the global financial system. Fueling trillions of dollars in illicit flows and money laundering activity were a range of destructive crimes, including an $782.9 billion in drug trafficking activity and $346.7 billion in human trafficking, as well as $11.5 billion in terrorist financing. In addition, fraud losses totaled $485.6 billion from a range of devastating fraud scams and bank fraud schemes, worldwide.

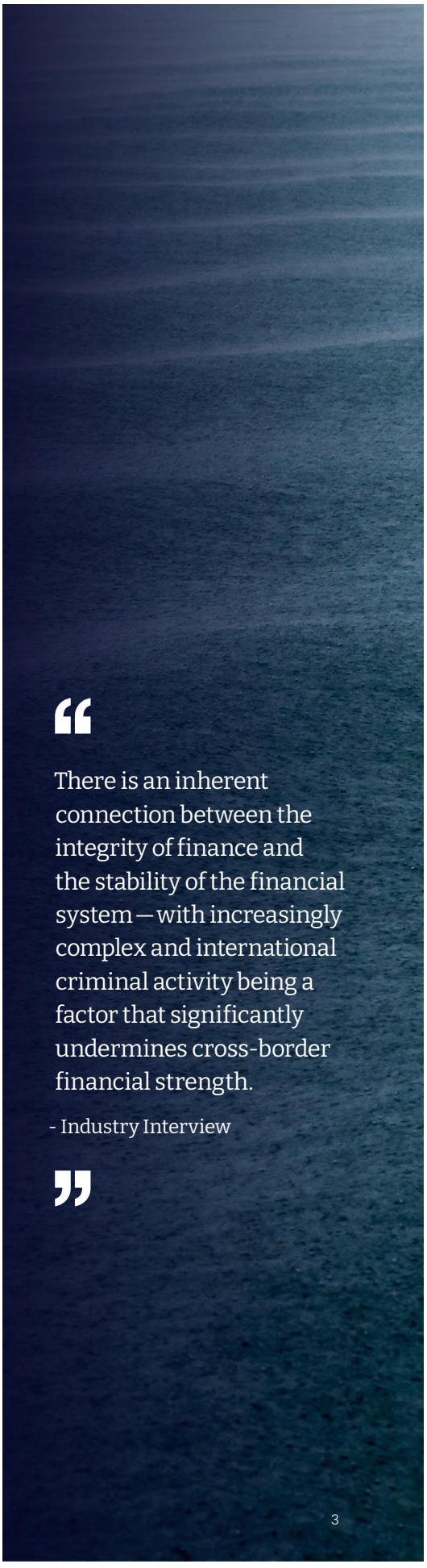
While the scale of these crimes is immense in value and impact, they can only be properly understood through the stories of those who survive them. The impacts are felt deeply in our communities and too often by the most vulnerable members of society. Throughout the report you'll read about several survivors whose stories shed a deeply incisive light on the human impacts of financial crime. Even with the emotional toll of their experiences and fear of judgement, these brave contributors came forward in the hope that their very personal stories provide greater understanding of these crimes — and help protect others from the same fate.

Adena T. Friedman
Chair & CEO

> "Ultimately, we know that no single company, industry, technology, or government is going to solve the complex problem of financial crime alone.
>
> We all have a responsibility — to ourselves and to the world — to be part of the solution."

The report also includes input from detailed interviews which reinforce recommendations about how the wider anti-financial crime ecosystem could collectively address the issues better. These recommendations include facilitating better collaboration among banks and with the public sector, increasing the implementation of new technology such as artificial intelligence, and more broadly, the need to evolve the regulatory framework to better support financial institutions in their efforts to prevent financial crimes.

Ultimately, we know that no single company, industry, technology, or government is going to solve the complex problem of financial crime alone. There is an opportunity to work together on a framework and align on measures of success for effective anti-financial crime programs. We all have a responsibility — to ourselves and to the world — to be part of the solution. Nasdaq has made the fight against financial crime central to our business, investing in cutting-edge surveillance, fraud detection, anti-money laundering technologies, and promoting public/private sector partnerships. Now, we look forward to facilitating a more global conversation about how we can collectively defend our financial system against the financial criminals seeking to exploit it.



> “There is an inherent connection between the integrity of finance and the stability of the financial system — with increasingly complex and international criminal activity being a factor that significantly undermines cross-border financial strength.”
>
> - Industry Interview

Table of Contents

About this Report

Last updated January 19, 2024

This report is based on data collection,[1] research and analysis performed by Celent Research and Oliver Wyman, as outlined in the methodology. A custom model was developed to determine the global estimate of financial crime, grounded in the best available industry data from public and private sources, market knowledge, and global economic patterns and indices. In addition, Celent Research and Oliver Wyman conducted a survey of more than 200 anti-financial crime professionals from financial institutions, as well as deep-dive interviews with senior executives, to inform the industry insights within this report.

Notwithstanding this expert research, we recognize that the scope of the model is not inclusive of all financial crime typologies and data is limited to current global detection and reporting capabilities and/or law enforcement interdiction — these numbers can only represent a fraction of criminal activity and victims of financial crime.

We especially acknowledge and thank Timea Nagy, Steve, Debby Montgomery Johnson, and Lilah Jones for their courage in sharing their lived experiences and providing insight into the human impact of financial crime.

Methodology

Global Estimates of Financial Crime

Financial crime estimates for fraud and money laundering were developed by Celent Research and Oliver Wyman. Estimates were built using a bottom-up amalgamation of regional and country-level estimates, which were then compared with top-down estimates from global sources. Global indices and data were used to create the regional and country-level estimates. Data sources include governments, international agencies, non-governmental organizations (NGOs), law enforcement agencies, interviews with industry experts, and news media.

The three-stage approach to developing these global estimates of financial crime included:

1) Bottom-up Modeling

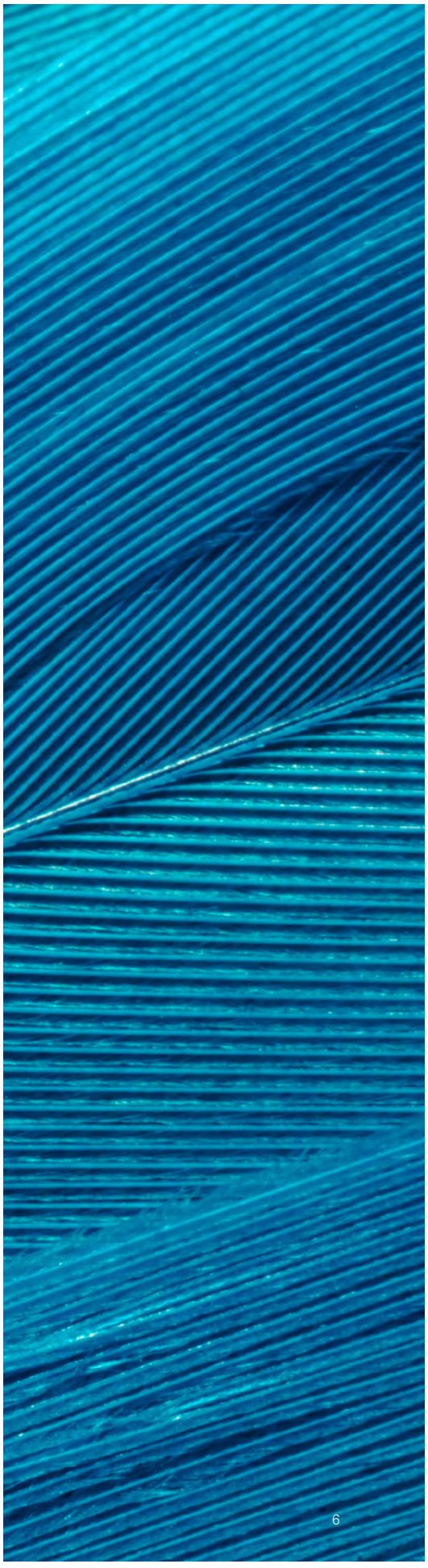
The foundation of the model was built on more than 450 global, regional, and country-level estimates and reports of fraud, financial crime and money laundering activity. These individual data points were combined and then extrapolated to fill in country-level and regional gaps. Estimates from prior years were adjusted to 2023 estimates.

Data sources for bottom-up modeling include, but are not limited to:

- **Governments and Law Enforcement** *(e.g. Australian Financial Crimes Exchange (AFCX), Australian Taxation Office (ATO), Canadian Anti-Fraud Centre, Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3), Japan's National Police Agency (NPA), Singapore Police Force (SPF), South Africa's Special Investigating Unit (SIU), the United Kingdom's Department of Health and Social Care, the United Kingdom's Home Office, United States Department of Justice (DOJ), United States Department of the Treasury)*
- **Private Sector** *(e.g. Deloitte, Euromonitor, FICO, The Harris Poll, McKinsey & Co., Oliver Wyman, LSEG Data & Analytics, S&P Global Data & Analytics)*
- **NGOs and Trade Groups** *(e.g. Association of Certified Fraud Examiners, Identity Theft Resource Center (ITRC), Ponemon Institute, World Bank)*
- **Media Sources** *(e.g. Financial Times, Forbes, AML Intelligence, Finbold, Regtechtimes)*

2) Top-down Modeling

The next step of the modeling process considered global estimates of fraud and money laundering to build a broader framework for the model. These data provided global totals for specific types of financial crime (e.g. human trafficking), different methods (e.g. trade-based money laundering) or for a category of financial crime as a whole (e.g. payment fraud).



Any data sets that were reported in a previous year were adjusted to 2023 levels for both economic growth and technological advances that abet financial crime. The data sources used for top-down modeling were primarily international agencies and NGOs *(e.g. Bank for International Settlements (BIS), International Monetary Fund (IMF), World Bank, United Nations).*

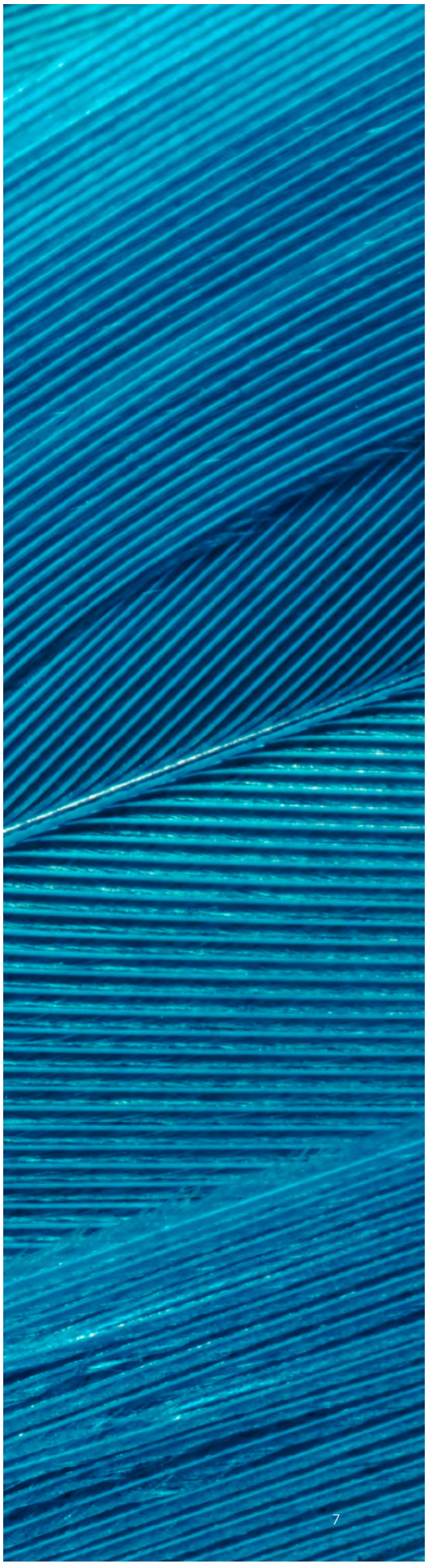
3) Reconciliation with Global Patterns

The final step in building the model was to reconcile the country, region, and global data. Global data and indices were used to rebalance country-level and regional estimates using economic data, financial data and global indices of criminal activity. Data for this part of the methodology were sourced from international agencies *(e.g. Global Initiative Against Transnational Organized Crime's Global Organized Crime Index and the Basel Institute on Governance's AML Index).*

Scope

Please note that the fraud loss estimates do not include tax evasion, corruption, bribery, embezzlement, business lost to counterfeit goods or industrial espionage. The regional allocations of loss to fraud victims represent the location of the victim, not that of the perpetrator. Money laundering estimates are estimates of money flowing into and out of the banking system, and do not reflect the value of funds moved physically or through digital currencies.

In addition to the financial modeling, Celent collected primary data on top priorities, concerns and approaches to fighting financial crime from an online survey of 209 anti-financial crime executives from bank and non-bank institutions in North America ranging from $10 billion to over $500 billion[2] in assets.



Executive Summary

Financial crime threatens the integrity and security of our global financial system. Its scale is immense in value and impact, but even more so when the real human consequences of these crimes are considered. The impacts are felt deeply in our communities, too often by the most vulnerable members of society — while its perpetrators hide in the shadows, evading detection by leveraging the interconnected nature of our global financial system and exploiting new and emerging technologies for their illicit benefit.

By bringing together expert research and data, industry perspectives, and the voices of survivors, this global report provides insights into the scope and impact of fraud and money laundering, as well as the crimes that underpin the flow of illicit funds around the world.

Financial crime is a **multi-trillion-dollar problem.**

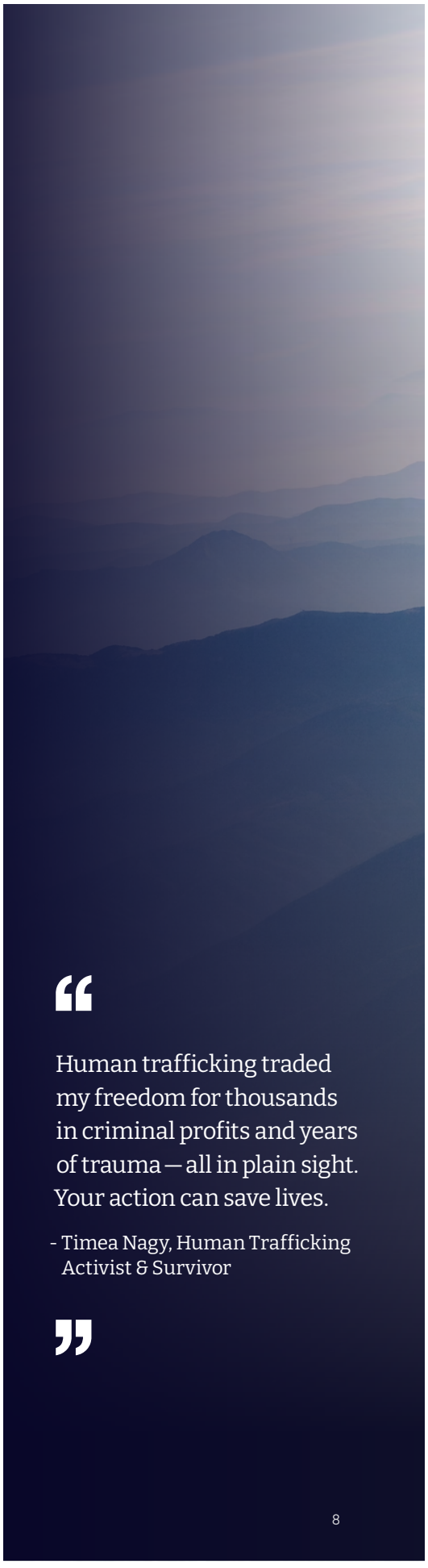
Last year alone, more than an estimated **$3.1 trillion** in illicit funds flowed through the global financial system.

Among the most prevalent crimes that fueled trillions of dollars in illicit flows and money laundering activity were a range of destructive crimes, including an estimated:

- **$782.9 billion** in drug trafficking activity
- **$346.7 billion** in human trafficking
- **$11.5 billion** in terrorist financing

Additionally, in 2023, fraud scams and bank fraud schemes totaled **$485.6 billion** in losses globally.

Importantly, despite the diligence underpinning this research effort, it is critical to acknowledge that this only represents a fraction of the true scope of financial crime. The true scale cannot be accurately measured in numbers, given how much crime goes unreported by victims and undetected in the current financial system.



> “Human trafficking traded my freedom for thousands in criminal profits and years of trauma — all in plain sight. Your action can save lives.”
>
> - Timea Nagy, Human Trafficking Activist & Survivor

The human impact of financial crime cannot be understated and can only be fully understood through the stories of those who survive it. Four courageous victims have contributed their experiences to this report, to help the industry learn from real survivor stories and underscore the need for change.

The industry is calling for collective action in the fight against financial crime. Financial institutions are investing significant time and resources to ensure they are compliant with their regulatory obligations, while also combating fraud and money laundering. Challenged by increasing operational costs, the inefficiencies of legacy systems and siloed approaches, there has been continuous strain on anti-financial crime programs' efforts to keep pace with new and evolving threats. To this end, the industry believes that financial institutions would benefit from more tailored regulatory guidance that elevates financial crime priorities, defines measures of program effectiveness, catalyzes the adoption of artificial intelligence (AI) and technology innovation, and advances information sharing efforts.

To protect the integrity of the global financial system and the communities it serves, there is a tremendous opportunity for governments around the world — working with the industry — to embrace greater collaboration, deploy innovative approaches, and provide better frameworks to halt an epidemic of financial crime.

The Global Scale of Financial Crime

From lone fraudsters to transnational criminal organizations,[3] criminals are not bound by borders, privacy, or the rule of law. They adapt readily as financial organizations implement new defenses — quickly leveraging new technologies for illicit purposes, sharing criminal best practices for profit, distributing their activities to evade detection, and ultimately perpetrating an estimated more than $485 billion in global fraud losses and fueling over $3.1 trillion in money laundering and terrorist financing worldwide.

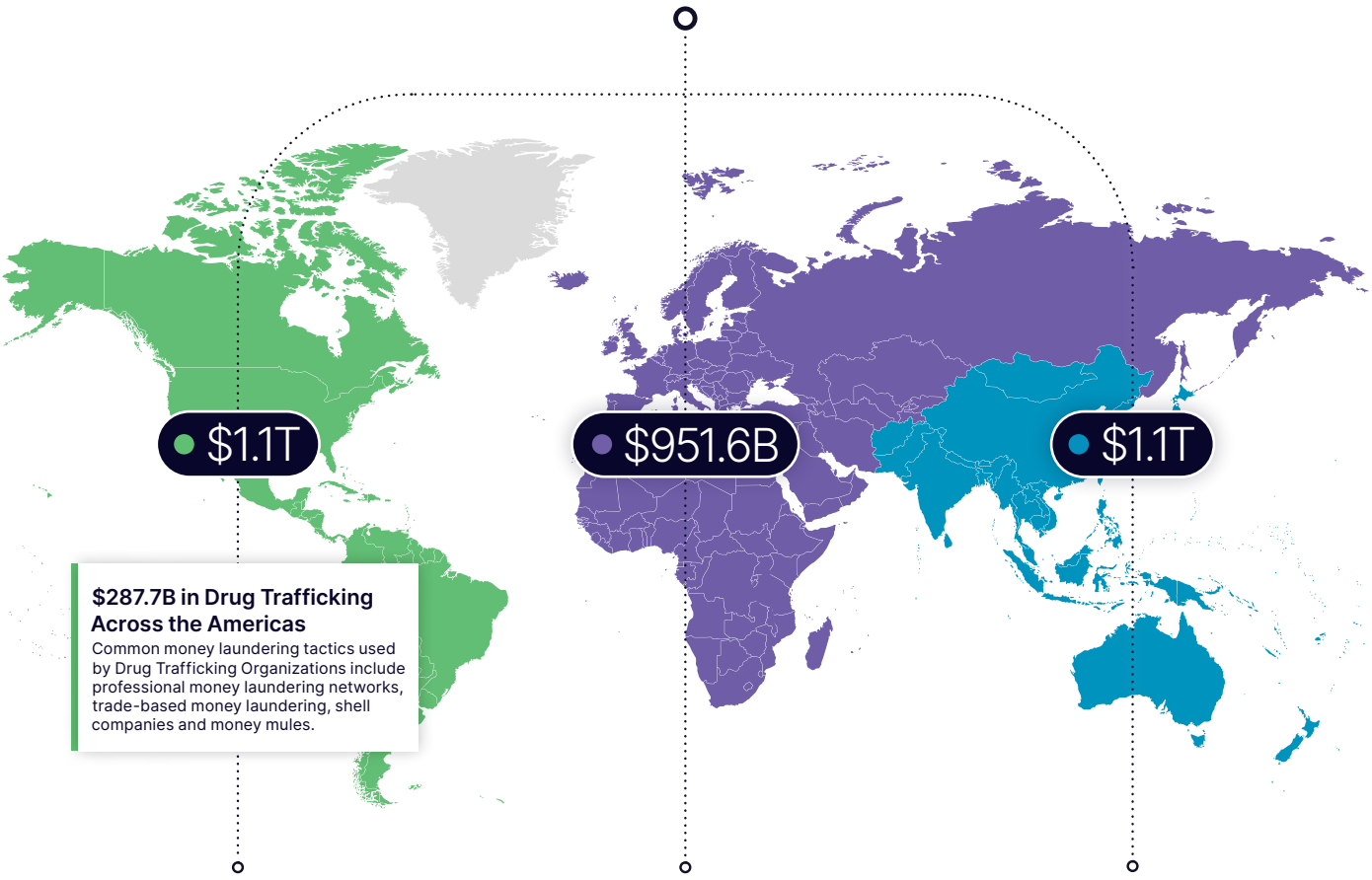
The scale of this global financial crime epidemic is immense. In 2023, globally, banks faced $442 billion in projected losses from payments, check and credit card fraud. Meanwhile, consumer scams touched every region, amounting to $43.6 billion in estimated losses that were shouldered by everyday people and businesses with potentially lifechanging consequences. In the last year, these fraud schemes, and heinous crimes such as human trafficking, drug trafficking and terrorist activity, fueled the flow of trillions of dollars in illicit funds through the global financial system.

The enormity of financial crime threatens the very fabric of our financial system and undermines communities everywhere. At the center of this grave injustice are the victims, whose stories of survival are essential to understand the impact of these crimes — and the pressing need for action.

The following global estimates were determined from a data model developed by Oliver Wyman and Celent Research, that was grounded in the best available industry data from public and private sources, market knowledge, and global economic patterns and indices.

$3.1 Trillion in Illicit Funds

Global estimate of terrorist financing, money laundering and the proceeds of underlying crimes including human trafficking, drug trafficking, corruption, organized crime, fraud and other illicit activity.



$287.7B in Drug Trafficking Across the Americas

Common money laundering tactics used by Drug Trafficking Organizations include professional money laundering networks, trade-based money laundering, shell companies and money mules.

Americas

- Other *(Organized crime, fraud, corruption, etc.)*..... **$653.4B**
- Drug Trafficking **$287.7B**
- Human Trafficking **$109.1B**
- Terrorist Financing..... **$5.1B**

EMEA[4]

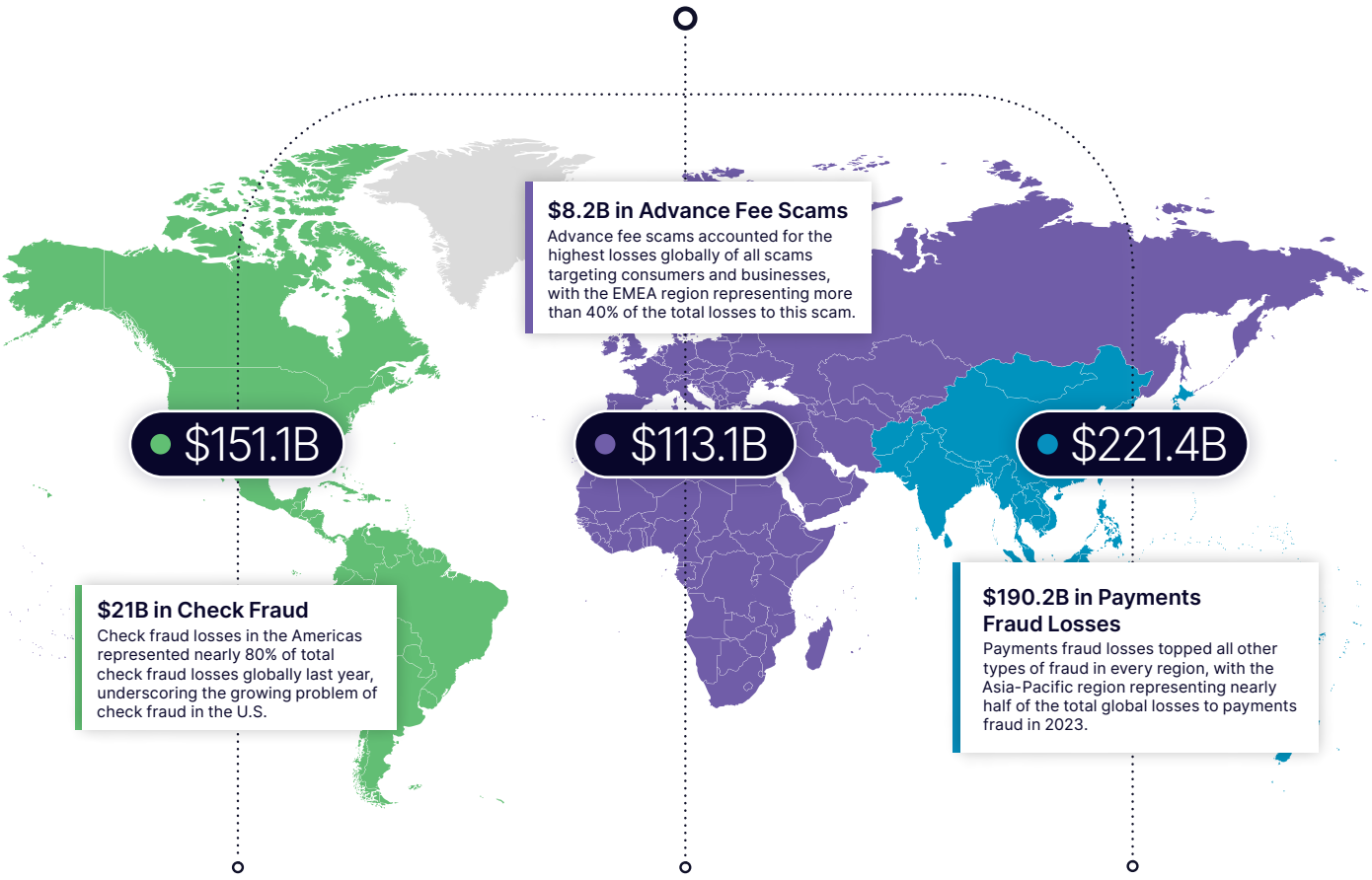
- Other *(Organized crime, fraud, corruption, etc.)*..... **$613.9B**
- Drug Trafficking **$226.4B**
- Human Trafficking **$107.6B**
- Terrorist Financing..... **$3.7B**

Asia-Pacific

- Other *(Organized crime, fraud, corruption, etc.)*..... **$690.8B**
- Drug Trafficking **$268.8B**
- Human Trafficking **$130.1B**
- Terrorist Financing..... **$2.7B**

$485.6 Billion in Scams & Schemes

Global losses to consumers and businesses from impersonation, confidence, advance fee, employment, and cyber-enabled scams, as well as bank fraud losses from payments, check and credit card fraud.



$8.2B in Advance Fee Scams
Advance fee scams accounted for the highest losses globally of all scams targeting consumers and businesses, with the EMEA region representing more than 40% of the total losses to this scam.

$21B in Check Fraud
Check fraud losses in the Americas represented nearly 80% of total check fraud losses globally last year, underscoring the growing problem of check fraud in the U.S.

$190.2B in Payments Fraud Losses
Payments fraud losses topped all other types of fraud in every region, with the Asia-Pacific region representing nearly half of the total global losses to payments fraud in 2023.

Americas

- Payments Fraud **$102.6B**
- Check Fraud **$21.0B**
- Credit Card Fraud **$13.6B**
- Cyber-Enabled Scams **$5.0B**
- Advance Fee Scams **$4.7B**
- Impersonation Scams **$1.6B**
- Employment Scams **$1.6B**
- Confidence Scams **$0.9B**

EMEA[3]

- Payments Fraud **$94.0B**
- Advance Fee Scams **$8.2B**
- Credit Card Fraud **$3.1B**
- Cyber-Enabled Scams **$3.1B**
- Employment Scams **$1.7B**
- Impersonation Scams **$1.4B**
- Confidence Scams **$1.2B**
- Check Fraud **$0.5B**

Asia-Pacific

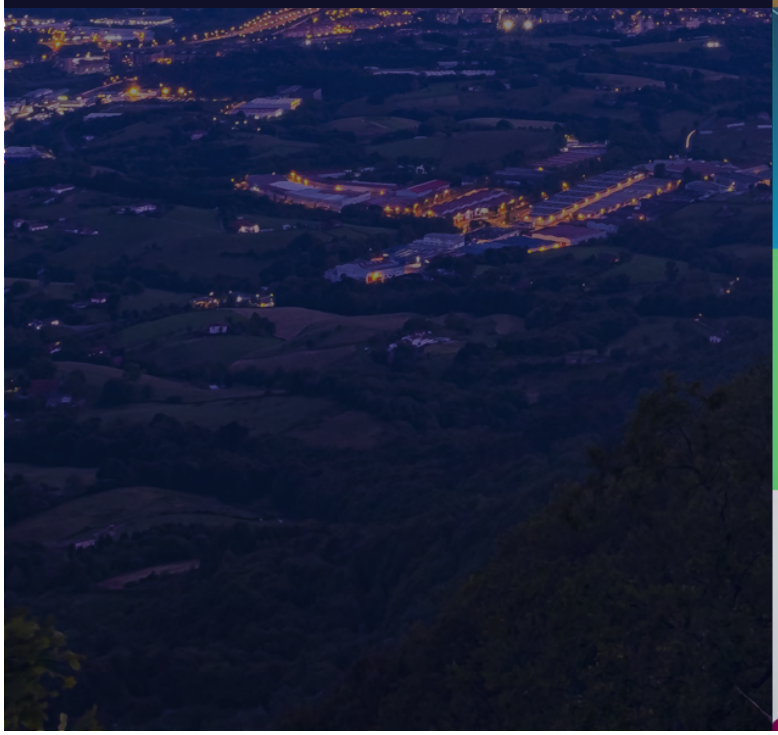
- Payments Fraud **$190.2B**
- Credit Card Fraud **$11.9B**
- Advance Fee Scams **$6.2B**
- Check Fraud **$5.1B**
- Impersonation Scams **$3.8B**
- Cyber-Enabled Scams **$1.9B**
- Confidence Scams **$1.7B**
- Employment Scams **$0.6B**

Survivor Spotlights

By any measure, the world's financial crime epidemic is immense. These numbers often overshadow the devastating impact of financial crime on everyday people—from lost livelihoods to lasting trauma. Representing only a fraction of people affected by financial crime globally, the following survivor spotlights provide a glimpse into the deep human impact of these crimes, and the lasting consequences for victims.

The report brings this reality forward, amplifies the voices of survivors and provides context to the industry insights with stories of lived experiences; ones that provide a deeper understanding of the impact of underlying crimes.

With first-hand knowledge of how criminals manipulate victims, and the financial and behavioral indicators of exploitation—survivor insights are invaluable for anti-financial crime efforts and can be critical inputs to improve solutions for effective prevention.



Lilah's Nightmare: When Business Email Compromise Jeopardized Her Dream Home

Lilah Jones
Sales Professional at Google*

At the altar, Lilah Jones pictured life with her new partner starting differently.

She spent New Year's Eve 2022 getting married in Puerto Rico and looking forward to what she knew would be a big year. As soon as she and her new husband got back home to Chicago, they would start searching for their dream home.

With interest rates still low but projected to rise, Lilah knew they needed to act fast. But she wasn't worried — as a mother, a motivational speaker, and a dynamic sales professional at Google, Lilah was no stranger to having a lot on her plate. She threw herself into the house-hunting process, and just a few short weeks later, they found it — their perfect house, with enough room for their kids and Lilah's mother who was moving in.

As they inched towards closing on the house, life got even more hectic. Lilah changed jobs and started coordinating her mom's move. All the while, she was keeping on top of all that goes into a home purchase: the inspections, underwriting, and the coordination between real estate agents, mortgage companies, and the title company.

"I wanted to make sure all of my ducks were in a row," Lilah said.

On the Monday before closing, Lilah received an email with the instructions for how to wire her down payment and closing costs to the title company. She'd been expecting this — she had reached out to the title company weeks before to confirm the process and ask what elements would be in the email.

Lilah checked the email closely: everything seemed as it was supposed to, and it came directly from the person she'd been dealing with at the title company. Even still, she wanted to be sure, so she called the title company to confirm the instructions. When no one answered or returned her call — and not wanting to jeopardize the closing that was 48 hours away — she moved forward with wiring the money from her bank on Tuesday.

The big day arrived on Thursday morning. Lilah and her husband sat at the closing table, nervous and excited about their big purchase.

Then, the title company agent came in with a stunning revelation: they hadn't received Lilah's $130,000 down payment.

Lilah was shocked. She grabbed her phone and pulled up the instruction email she had received. Almost immediately, the title company representative identified it as a spoofed email address. At first glance, the email looked like it had come from Lilah's contact at the title company. But clicking on the sender's name revealed another address that was so close to the original it was almost indiscernible.

The title company representative handed her a pamphlet on real estate transaction fraud and asked what she wanted to do.

"I couldn't believe it — I had no idea what to do in this scenario," Lilah said. **"Every eye in the room was on me, I felt sick."**

*The opinions expressed herein are solely those of the Interviewee and are not associated with Google in any way.

But there was no time to waste, so Lilah sprang into action. She waited for hours at her bank, hoping to stop the wire transaction. But she was told there was nothing they could do since 48 hours had passed. A call to local law enforcement was similarly unhelpful. Her focus then shifted to her top priority: saving their dream house.

Over the next few days, Lilah and her husband moved their money around and cobbled together a new down payment. With funding secured and the wire instructions triple-checked, they were able to reschedule their closing and took possession of the house the following Tuesday. Their relief was palpable.

But the joy from that happy moment was short-lived, as Lilah's attention soon returned to the Business Email Compromise scam that stood to cost her so much.

"I was sick of hearing, 'There's nothing we can do,'" Lilah said, **"I refused to be a victim."**

Lilah started doing a significant amount of research online and called everyone who could conceivably help her. Fueled by this tenacity, she eventually found a company that helps victims of wire fraud recover their money. The company's representatives offered the first glimpse of hope: there was a chance the stolen funds might still be sitting in an account somewhere. They promised to do everything to find it.

What you need to know:

While **Business Email Compromise (BEC)** scams occur less frequently against title companies than businesses and individuals, they are often extremely lucrative given the high value of real estate transactions.

Lilah's advice: "*If you're about to do a transaction where you're using a wire of any sizeable sum, anticipate a scam is about to take place.*"

A few days later, Lilah received good news. They had found her money, which was still in the criminal's account—an account that had now been frozen. Her bank would be able to recover her stolen down payment.

It took four months, but Lilah ultimately got back about $123,000. It was a rare happy ending for this type of real estate transaction fraud, one that Lilah doesn't take for granted.

> "Even if you become a victim of financial crime, you're not powerless. Be an advocate for yourself."

Spotlight:
Business Email Compromise

At the intersection of cyber-enabled fraud, consumer scams and payments fraud is Authorized Push Payment (APP) fraud, which has become increasingly prevalent in the financial industry.

Business Email Compromise[4] is an extremely lucrative form of APP fraud, where fraudsters direct their attacks against an organization, typically a business, and aim to intercept and redirect transfers of funds.

These scams are grounded in deceit — a fraudster posing as a genuine payee persuades a victim to transfer funds into an account under their control.[5] Losses to Business Email Compromise can be considerable and may extend to individual people who are transacting with the organization impacted by the fraud.

In Lilah's experience, the title company organizing her dream home purchase was compromised, leading to her property payment being stolen. In these scams, fraudsters typically favor irrevocable payment methods, such as wire transfers, to render recovery of the funds more difficult. Consequently, business wire fraud attempts have increased significantly in recent years.[6]

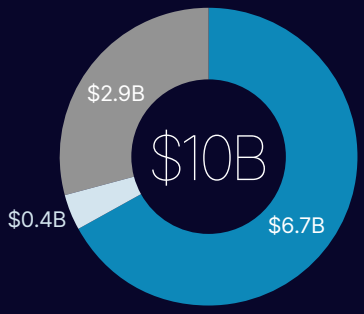
The growing sophistication of fraudsters in adapting to technology has increased the risk of these fraud scams on digital channels. Globally, over 15% of consumer fraud losses in 2023 were linked to Business Email Compromise — equating to an estimated $6.7 billion. All organizations are a target — from massive corporations to mom-and-pop businesses, government departments, non-profits, academic institutions and title companies.[7] It can cost individuals their lifesavings and homes, and severely impact the reputation and growth of an organization, devastating livelihoods.

Financial institutions are a critical first defense against the life changing consequences of APP fraud such as the Business Email Compromise scam that jeopardized Lilah's down payment. By dutifully monitoring for red flag indicators of these scams and deploying effective payments fraud analytics that use consortium data to consider payor and payee risk, financial institutions can interdict to prevent major losses before payments are sent.

> "Don't assume it can't be you. No matter what you do for a living, or where you are in your life or how efficient you think you are — nobody is above being scammed."
>
> - Lilah Jones on Business Email Compromise Scams

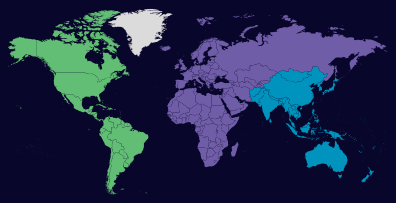
Banking on Deceit

$10B in Losses to Cyber-Enabled Scams



In 2023, 67% of cyber-enabled scam losses were a result of Business Email Compromise.

Business Email Compromise Represented $6.7B in Losses



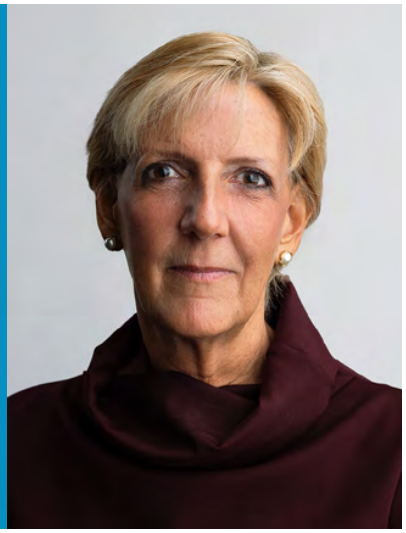
Americas:
$3.4B

EMEA:
$2.1B

Asia-Pacific:
$1.3B

of Survey Respondents Ranked **Business Email Compromise** As a Top Concern.

Debby's Heartbreak: The Romance Scam that Cost a Widow $1 Million



Debby Montgomery Johnson
65
Fraud Awareness Advocate

At 51, Debby Montgomery Johnson led a full life.

She and her husband, Lou, had been happily married for 26 years. They were both Air Force Veterans and she now worked at a bank, while he ran his own business. With one teenager at home, one in college, and two older boys serving as military pilots, Debby and Lou were just starting to envision what life might look like as empty nesters.

Then Lou suddenly died, and Debby became a widow overnight.

"I was so mad—at Lou, at the world," said Debby. **"None of it was part of our plan."**

But Debby didn't want the world to see her pain. Every morning, she woke up and forced a smile on her face, staying busy by taking over Lou's business. She only allowed herself to cry at night when she was back home alone.

Her friends were worried for her and encouraged her to try online dating. In time, she created an online dating account, hoping she could find someone to talk to—a companion to fill the void of loneliness.

Soon, someone caught her eye.

Eric was a British businessman, with a son of his own and a kind smile. He was widowed, like her. And as they began chatting, she quickly discovered that he was charming and could keep a conversation going. They started talking over instant message all the time.

"Every time I heard the chirp from my messaging app, I'd run over to my computer so we could keep talking," said Debby. **"It was like I was 16 again."**

As they shared more about each other, their families, and their lives, Debby grew to trust Eric—and with that came a sense of security. When she noticed small inconsistencies in Eric's stories, they were easy to rationalize, especially as the pair grew closer.

Just a few weeks after they started talking, Eric asked Debby for money for the first time.

It was such a small amount—just $50—that Debby didn't hesitate. It was only later she would realize it was a test—one she unfortunately passed. With promises of repayment, she was happy to help float him cash he needed to get by.

The requests for money slowly became more frequent, the dollar amounts creeping up over time. Debby became a fixture at Western Union and her banks, regularly sending thousands of dollars to places like Malaysia, England, and India—$2,500 here, $10,000 there. When she depleted her immediate savings, she tapped into her retirement accounts, sold jewelry, and even eventually borrowed money from her parents as the months ticked by. She kept meticulous records of all the money she sent to or on behalf of Eric, but she had no idea how much it was adding up to.

After two years, she had transferred more than $1 million dollars. None of it has been repaid.

"At the time, the stories he told me felt so urgent and made so much sense," Debby said. "It went on for so long—my accountant knew about him, my banker knew about him, my family knew about him. It had to be real."

But it wasn't. In September 2012, Eric came online and asked Debby, to her confusion, how she felt about forgiveness.

Then he confessed: their entire relationship had been a scam.

Debby immediately rejected the idea—it couldn't possibly be true. Eric turned on his video camera for the first time, revealing a young Nigerian man who bore no resemblance to the British widower she had received pictures of.

"It felt like hitting a brick wall," Debby said. As "Eric" apologized and tried to play on her sympathies to keep the relationship going, she was overwhelmed by feelings of anger and shame. Her mind began to spin with questions: *Could she catch him? Could she somehow get her money back?*

After closing out of the chat, Debby contacted the FBI, armed with more than 4,000 pages of journal entries and financial records from the past two years. Law enforcement confirmed the fraud, but there was little that could be done. The money was long gone, and there was little hope of finding and prosecuting the international perpetrators.

"Losing the money was obviously devastating," Debby said. **"But what's worse is what it does to your heart, your trust."**

What you need to know:

Romance scams are among the fastest growing frauds, affecting thousands of victims with millions in losses.[8]

Debby's advice: *"Slow down anytime someone comes to you with an emergency and asks for money. Scammers use urgency to get you to act before you think."*

In the aftermath of the fraud that defined two years of her life, Debby struggled to move forward. It fundamentally changed how she looked at the world, as she became wary of interacting online or with new people in her social circle.

She found a new sense of purpose by dedicating herself to raising awareness about the pervasiveness and risk of romance fraud and scams. She knows now that there's a full playbook criminals use to psychologically manipulate people into opening both their hearts and their bank accounts—and like her, they may never find justice.

> "People always think it could never happen to them—I know I did, and I'm a former intelligence officer. If it can happen to me, it can happen to anyone."

Spotlight: Romance & Other Consumer Scams

Confidence scams are often designed to exploit lonely or isolated people in their most vulnerable moments. Through lies and deceit, fraudsters will wholly dedicate themselves to gaining a victim's trust and abuse it for financial gain.

Romance scams epitomize this tactic, and the extreme measures fraudsters are willing to take to deceive their victims.

As in Debby's experience, romance scammers dedicate themselves to cultivating a fictitious relationship with their victim, often making contact through online dating sites or social media. Although initially amorous, the relationship becomes defined by escalating requests for funds, and ultimately considerable monetary losses and immeasurable heartbreak.[7]

Romance scams are among the fastest growing frauds,[9] with estimated losses of $3.8 billion in 2023 along with other confidence schemes. No statistics can capture the mental anguish and emotional consequences that victims of these scams experience. Even so, its perpetrators demand funds until the victim often has nothing more to give. They can be used as an unwitting money mule, moving funds for the fraudsters — without realizing they are laundering the profits of other crimes.[8] In many cases, victims may be unable to accept that the relationship is a scam, making intervention highly challenging.

Working directly with customers and members, financial organizations are a crucial frontline defense against romance scams and other fraud schemes. Vigilance and tactful inquiry can help uncover instances of potential exploitation at the earliest opportunity, leading to intervention that may be essential in protecting victims like Debby from devastating emotional and financial damage. Utilizing innovative anti-financial crime solutions that profile both the sending and receiving accounts of funds transfers can also allow financial institutions to ensure transaction activity is typical for both parties.

> "You're so invested — heart, mind, and soul in this person, and you really believe that they are who they are. Until you find out that they're not."
>
> - Debby Montgomery Johnson on Romance Scams

Emotional Exploitation

Romance scams are among the world's **fastest growing fraud trends.**[9]

Romance scams caused

$3.8B

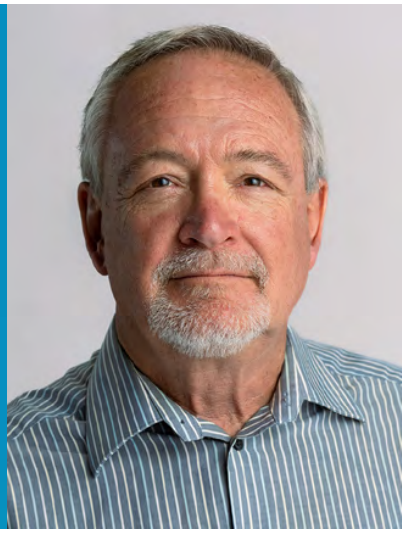
in estimated global losses with other confidence schemes.

Romance Scams represent a fraction of the losses to consumer scams but the **toll on victims is immense.**

> "My heart got ripped out. And my trust in people was really challenged."
>
> - Debby Montgomery Johnson on Romance Scams

Steve's Struggle: How Scammers Exploited this Semi-Retired Scientist

Steve
68
Scientist, Artist & Stanford Graduate



The golden years were just starting to come into focus for Steve.

A Stanford graduate, he'd built an accomplished career as an applied scientist, even hosting a podcast that combined his love of agriculture and pop culture. But at 68, he was looking forward to a slower pace, with more time for his passions like gardening, hiking near his home in San Diego, and artwork inspired by botany, biology and the flora that defined his career for so long.

Steve wasn't quite ready to call himself fully retired, though. He was still doing some consulting and freelance writing out of his home office. So, when he received an invoice from the Geek Squad on a Friday in 2022, he didn't think anything of it. He had a service contract for his computer, and he knew it was up for renewal soon. But the amount of the invoice—$399—was higher than expected.

"It looked like every other Geek Squad email I'd ever gotten," Steve said. He called the customer service number conveniently listed in the email.

Steve reached a friendly agent, who confirmed the invoice was incorrect and that he would receive a full refund. Steve just needed to download a diagnostics app, so the agent could help him fill out the necessary paperwork. Once again, Steve thought nothing of it—it was common for the Geek Squad to request remote access as part of the troubleshooting process.

There was just one problem:
he wasn't talking to the Geek Squad.

When Steve downloaded the app, criminals got full access to his computer and everything on it. They used it to access his bank accounts, move his money around, and make it appear that $20,000 had mistakenly been deposited into his account.

Now the real scam was in motion.

The agent began talking about how much trouble he would get in for the mistaken transfer. He would need Steve's help to fix things, by initiating a wire transfer to return the money.

"It was impossible not to feel bad for the guy," Steve said. **"I wanted to help."**

Steve set out for his local bank branch. But when he got there, they wouldn't authorize the transaction. The scammers wouldn't be deterred. With the wire transfer off the table, the agent told Steve he could withdraw cash from the bank and use it to buy gift cards.

While he still felt sympathetic toward the agent, Steve began getting suspicious. He started asking more questions about who he was talking to, the transaction, and the gift cards.

Soon, the scammer's tactics changed: friendliness gave way to threats that his entire bank account could be shut down if he didn't comply.

Worried that he was being blackmailed and could lose all the money in his account, Steve withdrew $12,000 from the bank. When the teller at the bank asked what the money was for, Steve said it was to pay for home renovations—the lie supplied by the scammer.

What followed was a nightmarish weekend. With stores limiting how many gift cards can be purchased in a single day, Steve scrambled around San Diego trying to find new places to buy cards. All the while, the scammer just kept calling, demanding more money as quickly as possible.

He began to fear that they would never leave him alone.

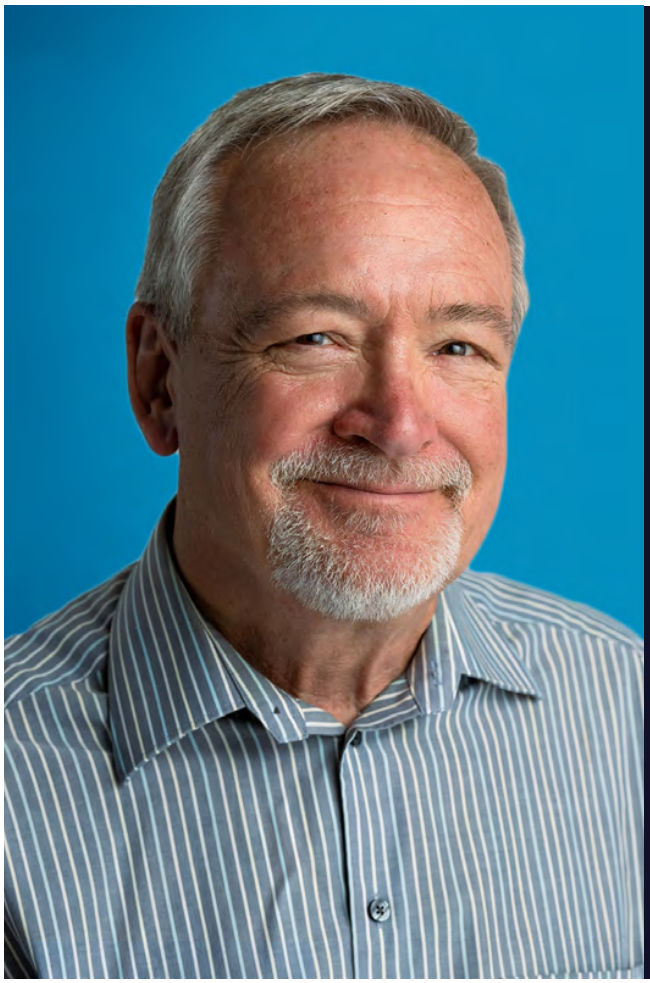
When Monday morning finally arrived, Steve went back into his bank and told them everything that was happening. They confirmed his worst suspicions: he was the victim of a fraud scam. Steve contacted law enforcement, but the damage was done.

None of Steve's $12,000 was ever recovered, and no one was apprehended for the crime.

What you need to know:

Elder abuse is vastly underreported but is estimated to **impact 1 in 10 elderly Americans each year.**[9]

Steve's advice: *"Trust your gut. If something doesn't feel right, take a breath and talk to somebody else about your situation."*



Steve debated sharing his story for a long time. He did not feel comfortable sharing with his friends, family or in his professional circles that he had been duped by this type of scam. Even today, he shoulders a sense of responsibility for what happened and is worried about being taken advantage of again.

While he ultimately decided to step forward to help others learn from his experience, Steve is eager to focus on his retirement, artwork, and passions in life — and leave the events of the scam behind. It's a common sentiment among victims of financial crime, particularly older adults, or seniors, who often don't report exploitation and fraud.

> "If sharing my story keeps this from happening to someone else, it's worth it."

Spotlight: Elder Fraud

Fraudsters will exploit anyone they consider vulnerable — including older adults who they may perceive as isolated, less familiar with technology, or challenged by disability.[10]

Elderly individuals who are targeted in fraud scams are often persuaded to transfer funds under false pretenses for a benefit they will never receive. These financial crimes targeting seniors are often referred to as elder financial exploitation (EFE).

As in Steve's story, scammers may impersonate a person in a position of trust or extort funds through fear tactics. In grandparent schemes, another example of a financial crime targeting seniors, a scammer impersonates the victim's grandchild requesting financial aid in a crisis.

Financial exploitation and other forms of abuse impact an estimated 1 in 10 elderly people in the U.S. alone.[10] In 2023, $77.7B of the total losses was fraud against elderly victims — and despite the prevalence of this devastating crime, for every known case of elder abuse, it is estimated that 23 cases are never reported.[10]

Seniors who are exploited often do not report the crime to authorities out of shame, uncertainty of who to turn to, or simply a desire to leave the experience behind. But from lost retirement savings to emotional damage, fraud and financial exploitation can leave victims with lasting consequences and trauma.

With many senior victims unable or unwilling to come forward, financial organizations play a crucial role in detecting elder fraud and preventing exploitation. By diligently monitoring for indicators of potential exploitation during customer interactions and ensuring timely reporting of cases to law enforcement, financial institutions can prevent serious financial loss and emotional harm and protect seniors like Steve. Effective anti-financial crime solutions can also determine when a customer's activity is uncharacteristic and indicative of potential elder abuse, allowing anti-financial crime professionals to intervene before it is too late.

Preying on the Vulnerable

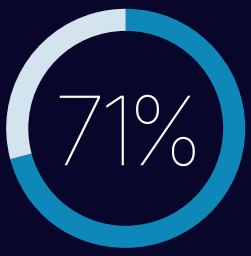
Seniors may be more at risk to fraud.

Of all reported global fraud

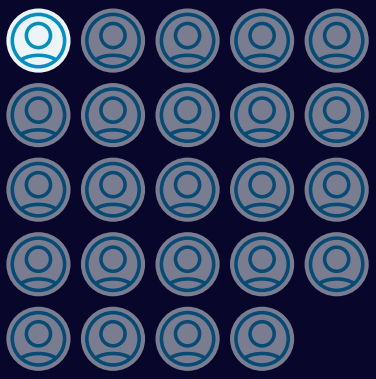
$77.7B

was linked to **elderly victims.**

According to Nasdaq Verafin Cloud data

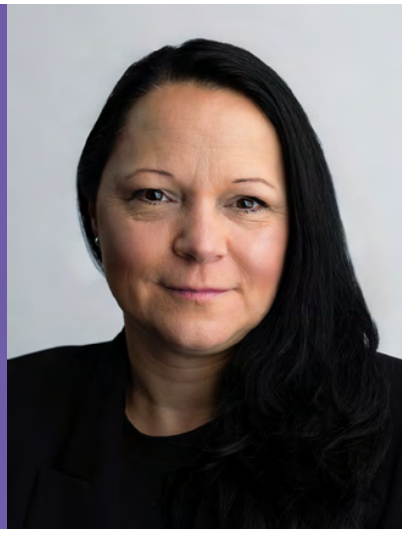


of wire fraud attempts targeted **people aged 55 or older** in Q2 2023.[7]



23 **unreported cases of elder abuse** for each known case.[10]

Timea's Journey: From Human Trafficking Survivor to Global Advocate



Timea Nagy
Human Trafficking Activist & Survivor

Growing up in Budapest, Hungary, Timea Nagy had big dreams and the work ethic to make them a reality.

At just 13 years old, she started working in film and TV. By 16, she had started her own production company — and at 20, she was already thinking about ways to grow the business. But as time went on, revenue declined. With mounting debt, Timea came across an opportunity that was too good to pass up.

She had found a newspaper ad from a recruiting agency seeking young women to work as babysitters and housecleaners in Canada. It was a three-month job paying $1,500 a month, a huge amount for Budapest in 1998. With that kind of money, she could pay her debt and help her family, as well.

"I was so desperate to make it work," Timea said. **"I had no doubts about it being a legitimate job. I was very naïve."**

Timea arrived in Toronto with a plane ticket paid for by the agency. She was picked up at the airport and driven to a motel.

That's when she found out the job ad was a front for something far more sinister.

"They said they were with the Ukrainian-Hungarian mafia, and I owed them a lot of money for my trip from Hungary. I would have to work as a stripper to pay off my debt—and if I refused, they would kill my family back home," Timea said. "This was all within six hours of getting off the plane."

Timea didn't see any options. The traffickers had confiscated her passport and threatened her and her family. She had no money, and she didn't speak English.

With nowhere to turn, she was forced to work as a stripper and a sex worker.

The days began to blur together. Timea and the other women under the traffickers' control were driven from the motel to seedy nightclubs around Toronto, where they spent hours working before being shuttled back to the motel with their one meal of the day—usually fast food.

"We were prisoners, starving and scared," Timea said. **"I worked every day for three months straight. I made them more than $40,000 in cash, and it still wasn't enough. They said I still owed them more money."**

Looming over everything was a constant threat of violence and abuse. In the worst moments, Timea found herself relying on the same coping mechanism she had developed as a child: closing her eyes and talking to herself. She would think: *It will be okay.*

Timea knew she had to make an escape plan. She realized that while her captors would drop her off at the nightclub she worked in, they would never actually come inside. This was her opportunity.

Using a dictionary she found, Timea began communicating with the security guards at the club.

She pointed to words like *help, escape, trouble, scared.* When the guards understood what was happening, they were horrified and agreed to help.

One day, when the traffickers dropped her off at the club, a security guard ushered Timea through to the back, where a car was waiting to take her to an apartment where she could hide. While the traffickers came close to finding her, she was able to make it on a flight back to Hungary two weeks later.

"I had no plan. I just wanted to feel safe, sleep, breathe," Timea said. **"I didn't want to feel like a sex object anymore."**

But Budapest didn't provide the relief she was hoping for. Timea found herself on the run from the mafia, who wanted to kill her, and the police who wanted to charge her with using a fake passport to get back in the country.

Knowing there was no safe future for her in Hungary, Timea said goodbye to her family and flew back to Canada on her own terms, moving in with the one friend she had made after escaping her captors. She struggled to pick up the pieces of her broken life.

"I was robbed of my youth," Timea said.

What you need to know:

Human trafficking is often a predicate offence to money laundering. Passing through victims, family members, associates and businesses, the illicit proceeds of this crime are obfuscated as a means of evading detection.[11]

Timea's advice: *"The traffickers who captured and exploited me had been operating for years before I was recruited. If someone had recognized the financial patterns and shut them down, my whole life would be different."*

It took decades for Timea to feel safe and heal the scars that remained from being trafficked. But she has refused to let her suffering be in vain.

Timea is now a human rights activist dedicated to eradicating human trafficking and supporting human trafficking survivors, even serving as an advisor to the United Nations on the subject. As she travels the globe sharing her story, she reminds people that everyone has a role to play in combating trafficking.

> "Human trafficking plays out in plain sight every day. Knowing the signs can save lives."

Spotlight: Human Trafficking

Human trafficking is modern slavery—and among the most heinous crimes imaginable.

Sex trafficking and forced labor are two major forms of human trafficking, which together generated over $346.7 billion in proceeds worldwide—with far more likely going undetected.

Traffickers commodify innocent people for illicit gain, resulting in the exploitation of millions of victims annually. At any given time, tens of millions of people are coerced into labor or sex work, generating massive profits for their traffickers.[12] As in Timea's experience, many victims suffer in plain sight but are never identified by authorities—escaping on their own with scars that last a lifetime.[13]

19% of our survey respondents called out human trafficking as a top threat, and two of the anti-financial crime professionals who participated in deep dive interviews stressed modern slavery as a significant financial crime risk.

The financial system can play a key role in identifying trafficking activity, providing intelligence to law enforcement, and aiding prosecution of traffickers. Banks that leverage modern technology, including AI, to parse through millions of financial transactions to track specific behavioral patterns and practices that are common among human traffickers, known as typologies, are advancing their ability to expose the criminals. Following the money can help expedite a victim's escape from slavery, prevent further trauma, and disrupt criminals that commoditize human beings for profit.

> "One of the most striking behaviors to look for in a victim of human trafficking is not the presence of a life being lived, but the absence of one. The trafficker takes everything they have. But it doesn't have to be that way."
>
> - Timea Nagy, Human Trafficking Activist & Survivor[12]

A Humanitarian Crisis

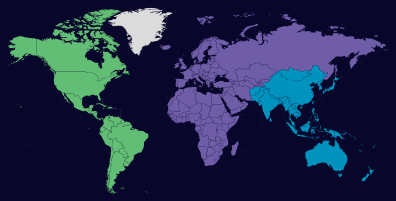
At any time, **tens of millions of people are coerced into labor or sex work.**[13]

In 2023, an estimated

$346.7B

of illicit funds was linked to **Human Trafficking.**

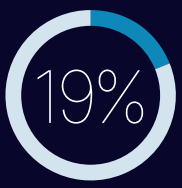
Human Trafficking by Region



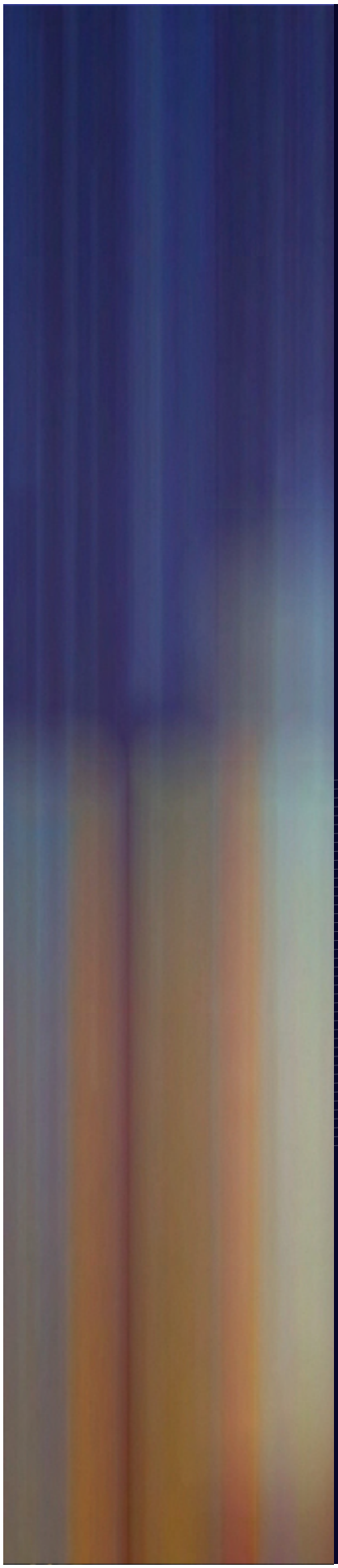
Asia-Pacific: **$130.1B**

Americas: **$109.1B**

EMEA: **$107.1B**



of Survey Respondents ranked **Human Trafficking as a Top Concern,** and in deep dive interviews it was elevated as a top concern.



Industry Insights

At the front line of preventing financial crime, financial institutions play a critical role in protecting the integrity and security of our global financial system.

Through our survey with more than 200 industry professionals and interviews with three senior anti-financial crime executives, this report brings industry insights forward to elevate the key trends, challenges, and opportunities facing financial institutions in their commitment and efforts to fight financial crime more effectively.

Industry Insights: Threats & Trends

The ability of financial institutions to manage evolving and emerging threats is paramount to protecting the integrity and security of our global financial system—and ensuring the trust of the communities we serve.

Financial institutions take a multi-pronged approach to keep pace with emerging trends. From law enforcement communications to industry working groups, or collaborating directly with other institutions, organizations rely on sourcing information from across various industry stakeholders to learn of new financial crime risks.

In our survey, anti-financial crime professionals prioritized the threat of fraud on real-time and faster payments systems, as well as complex typologies, such as money mule activity, global drug trafficking and terrorist financing. In our deeper dive interviews, two out of three professionals named human trafficking a top threat within their institution.

Fraud On Payments Channels

Respondents echoed shared concerns over payments fraud including real-time and faster payments fraud, government benefit fraud, elder abuse or exploitation and scams targeting consumers. Real-time and faster payments fraud was considered the top emerging threat, given that the adoption of these systems comes with many unknowns for anti-financial crime programs. As customer expectations for fast, frictionless transactions increase, so does the risk for fraud. With the ability to move funds instantly or nearly-instantly, these channels may accelerate consumer scams and fraud, as well as the flow of funds to and from mule accounts.

Money Moved Through Mules

Money mules are instrumental to financial crimes, acting as witting or unwitting conduits between fraud and money laundering. Their activities obfuscate criminals' identities and their sources of funds, facilitate the deposit and flow of illicit proceeds around the world, and aid in funding heinous crimes such as terrorist financing—all while evading AML/CFT controls and regulatory scrutiny. Often connected to larger mule networks and criminal organizations, detecting and disrupting money mule activity is crucial to interrupt the world's $3.1 trillion money laundering problem.

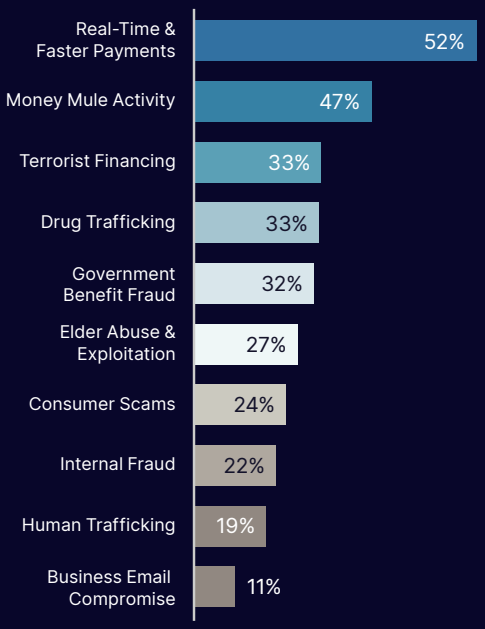
Methods to Stay Ahead of Emerging Threats:

56% Communications, alerts and reports from law enforcement agencies.

54% Participating in industry-wide initiatives and working groups.

50% Sharing information directly with other financial institutions.

Financial Crime Threats of Greatest Concern:



Countering Terror

From lone extremists to small cells and massive networks, financing is the lifeblood of terrorism. These funds are used to recruit, train, pay and mobilize members, promote radical ideologies, procure weapons, and execute attacks. By abusing the financial system, terrorists can obfuscate the flow of funds that support their nefarious activities. Globally, it is estimated that funding for terrorist acts and organizations amounts to $11.5 billion, including arms trafficking, foreign and domestic terrorism, and domestic violent extremism.

Terrorism threatens the safety and security of communities worldwide and tears at the fabric of society. Disrupting the financing flows to terrorist groups is essential to shut down these operations and the power they seek to gain from fear.

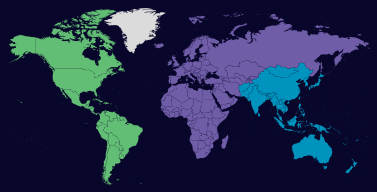
Drug Trafficking Operations

Trade in cocaine, opioids and heroin, methamphetamine, and other illicit substances is a multi-billion-dollar industry for traffickers and Drug Trafficking Organizations (DTOs). From producers to smugglers and dealers, drug-related activity crosses international boundaries to arrive on the streets of communities around the world. DTOs launder their proceeds through various illicit means including professional money laundering networks, trade-based money laundering, shell companies and money mules.

Globally, an estimated $782.9 billion was linked to drug trafficking and DTOs in 2023. Beyond generating billions, DTOs are often linked to violent crimes, and fuel substance abuse and addiction, with destructive and lasting effects on our communities. Intercepting the flow of funds to and from these activities is crucial to exposing and disrupting these criminal enterprises.

of Survey Respondents ranked **Terrorist Financing as a Top Concern.**

of Survey Respondents ranked **Drug Trafficking as a Top Concern.**



In 2023, an estimated

$11.5B

linked to

Terrorist Financing

Americas:

$5.1B

EMEA:

$3.7B

Asia-Pacific:

$2.7B

---

in 2023, an estimated

$782.9B

in Global Drug Trafficking/DTOs

Americas:

$268.8B

EMEA:

$226.4B

Asia-Pacific:

$287.7B

Industry Insights: Priorities in the Fight Against Financial Crime

A confluence of factors — including the scale and complexity of financial crime, the pace of innovation driving new threats, and the complexity of global regulatory frameworks — has resulted in an increasingly complex and costly environment for financial institutions who are at the forefront of fighting financial crime. Across the financial sector, financial crime is widely recognized as a key priority — commanding significant investments and resources, which are necessary to address the significant obstacles that remain in the fight to root out crime more effectively.

Our data reveals that financial institutions place a high priority on financial crime prevention but face significant challenges in keeping pace with burdensome and at times conflicting regulatory obligations and the evolving financial crime threat landscape — all while managing increasingly inefficient compliance processes, contending with limitations of legacy technology, and navigating increasing operational costs.

People, Process & Technology Limitations

Banks are increasing their investment in anti-financial crime programs to ensure they meet regulatory obligations, while also navigating evolving fraud threats and an increasingly complex financial crime landscape.

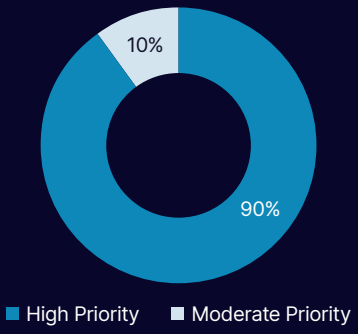
Nearly half of anti-financial crime professionals cited a lack of adequate resources and technology to fight financial crime — and this despite 75% of respondents reporting an increased investment in headcount in 2023 compared to the previous year.

Most respondents further noted that the limitations of their current anti-financial crime capabilities would necessitate substantial changes to their systems and processes.

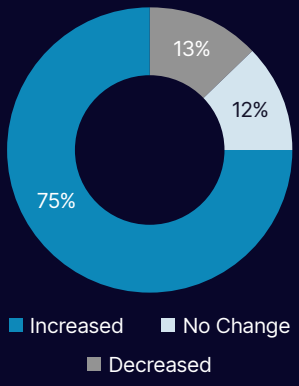
Legacy technology and processes further exasperate the limitations of current anti financial crime capabilities and increasing operational costs, due to:

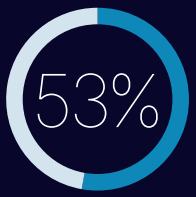
- Volume of False Positive Alerts from Rules-Based Systems. The sheer volume of false positive alerts generated on low-risk activity by broad, rules-based systems can result in the need for additional investment in personnel, increase customer friction, and focus time and resources away from higher-risk activity and investigations.
- Inefficiency of Manual Processes. Due to complex and often disconnected systems and data sources across financial institutions, daily workflows are often fraught with manual tasks, processes, and documentation requirements. Lack of automation can impact time to investigate, record-keeping, reporting, and other critical compliance processes, which can lead to increased operational costs and headcount.

Priority Placed on Financial Crime Prevention



Anti-Financial Crime Headcount: 2023 vs. 2022





of respondents said they have **adequate resources, including personnel and technology** to combat financial crime.

These factors can significantly impact a financial institutions' ability to keep pace efficiently and effectively with financial crime risks, while ensuring compliance with regulations.

Lack of Measures for Success

In the absence of clear guidance from regulatory authorities on priorities or measures for evaluating the effectiveness of anti-financial crime programs, along with completion of compliance training and time to investigate, the number of SAR/STR filings is the most common measure of effectiveness noted by respondents.

Without context of the value of the intelligence provided within reports or their usefulness to law enforcement, such as through feedback loops between the public and private sector—the count of reports filed cannot accurately reflect the true effectiveness of anti-financial crime programs.

Ongoing feedback from law enforcement directly to financial institutions on the outcome of reports filed would provide valuable input to anti-financial crime programs and measures of effectiveness, as well as timely insights into current threats.

Concerns for the Future

As financial institutions look to the future, ensuring regulatory compliance and keeping pace with financial crime risks are top priorities.

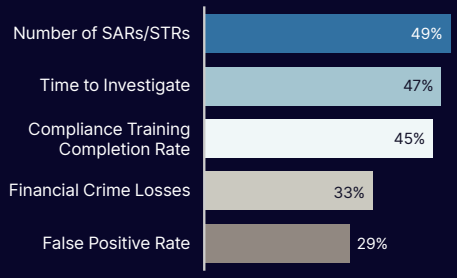
Financial institutions are working to manage a careful balancing act between adjusting to evolving regulatory obligations while allocating appropriate human and technological resources to ensure compliance—with significant financial implications for financial institutions.

In the face of these challenges, most respondents are pursuing technology, such as new solutions, AI, data and analytics to improve their efficiency and amplify their financial crime prevention efforts.

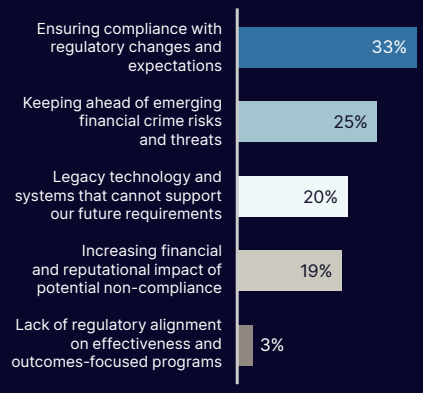
> "We are all missing activity because of a lack of integration with other financial crimes programs."
>
> - Industry Interview

> "We need a technology solution to the increase in volume. We can't continue to hire."
>
> - Industry Interview

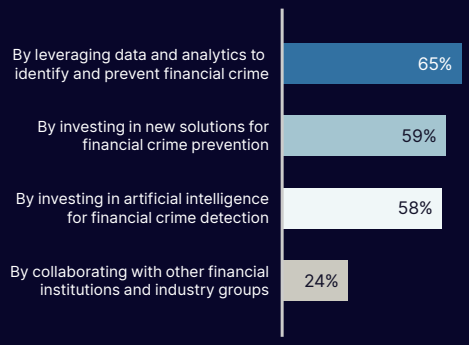
Current Measures of Program Effectiveness



Challenges of Greatest Concern: 5- to 10-Year Outlook



Opportunities for Improved Financial Crime Prevention with Plans to Pursue



Industry Insights: Opportunities

The financial industry believes there are significant opportunities for improvement and increased effectiveness. Most respondents pointed to substantial changes to existing systems and processes as key current or near-term priorities for their organizations. Financial institutions also underscored the need for greater clarity and guidance from regulators in many areas to advance their efforts to fight financial crime.

Improved Regulation

Regulatory clarity and guidance are crucial in enabling the industry to align priorities and fight crime more effectively. Respondents felt that improved regulation would benefit their anti-financial crime efforts in several critical areas, with most noting the value to their organizations when:

- Prioritizing specific financial crime typologies, such as human trafficking or drug trafficking detection, each of which have unique characteristics
- Encouraging information sharing, across financial institutions and with the public sector
- Supporting innovative technology, including AI

Embracing Collaboration

Both private-to-private and public-to-private collaboration models are seen as key areas that could drive greater effectiveness in crime fighting efforts. Criminals are leveraging siloes within an institutions' walls, as well as between institutions and between the industry, regulators, and law enforcement to evade detection. Financial institutions noted a need for greater alignment within their institution, to break down siloes between teams and departments, protect customers, and combat financial crime holistically.

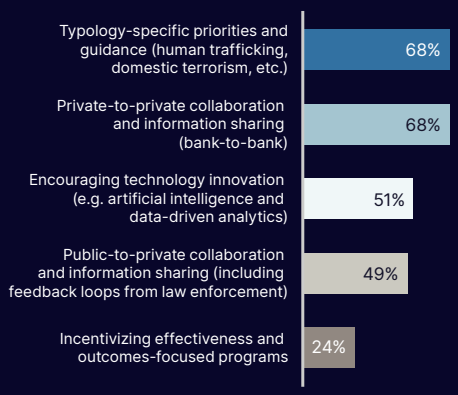
Respondents also underscored the importance of industry collaboration and information sharing as a strategy to defend against financial crime threats and stressed the need for regulatory guidance for public-private partnerships, as well as private-private information sharing between banks. Interviewees echoed this stance and emphasized the crucial role of advocacy groups in encouraging government agencies to focus on collaboration and public-private dialogues. Notably, one interviewee acknowledged that the public-private partnership known as Project Shadow[15] had been the impetus for implementing more robust monitoring for human trafficking at their organization.

> "Most banks rely on regulators to see what is on their list of priorities."
>
> - Industry Interview

> "Siloing is so detrimental to overall effectiveness of financial crime programs."
>
> - Industry Interview

> "We have put in place certain identifiers that trigger alerts for human trafficking as a result of Project Shadow."
>
> - Industry Interview

Areas for Improved Regulation



Innovating with Technology

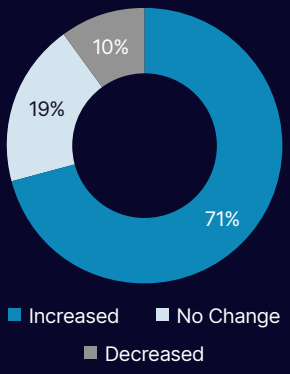
As financial crime evolves, capitalizing on technology opportunities is crucial. Although most respondents said their organization had increased its technology spend in 2023, the need for improved processes and systems and addressing challenges associated with legacy systems were common concerns.

Many anti-financial crime programs are weighing the benefits that adopting AI techniques could provide for efficiency and effectiveness, with respondents viewing transaction monitoring, Know Your Customer (KYC), and sanctions as the areas of greatest potential impact. While there is no clear guidance from regulators on AI, many institutions have implemented some form of AI techniques in their anti-financial crime programs, including intelligent document processing, natural language processing, robotic process automation (RPA) and machine learning, while only a quarter use generative AI or large language models (LLMs).

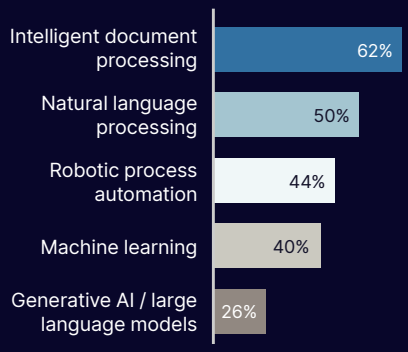
Most respondents expect their organization to increase spending on AI or machine learning in the next one-to-two years. Those considering generative AI will be deploying it to alleviate the complexity of daily processes on their workforce. This includes using the technology to examine beneficial ownership information (58%) and to enable financial crime analyst co-pilots (56%), for alert explanation/narrative generation (55%), or compiling and analyzing customer risk profiles (54%).

As compliance pressure mounts and financial crime evolves, organizations that do not plan to increase spending on AI will need to identify alternative means to strengthen their financial crime management programs.

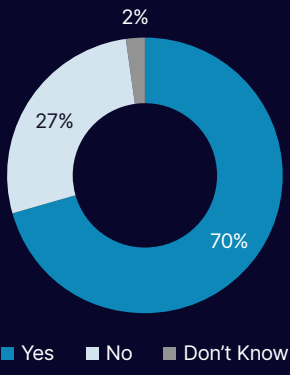
Budget for Financial Crime Compliance Technology (IT & Operations): 2023 vs. 2022



Technologies in Production for AFC Processes



Increase Spending on AI/ Machine Learning Technology: Next 1-2 Years



Pressing Need for Action

The world's multi-trillion-dollar financial crime epidemic is more than a money problem. It has profound human costs from despicable crimes that have a deep and lasting impact on the communities we serve.

To protect the integrity of our financial system—collective action is needed in the fight against financial crime.

Consider the Human Costs.
Behind the monetary toll of financial crime is a humanitarian crisis. By rethinking financial crime as a human problem, survivor experiences can inform industry-wide priorities and technology solutions.

Innovate Ahead of Evolving Crime.
As financial crime increases and criminals adapt, the industry cannot keep pace with added resources alone. By adopting new technologies and seizing opportunities for innovation, we can move towards more efficient and effective prevention.

Collaborate to Break Down Siloes.
The world's multi-trillion-dollar financial crime problem cannot be tempered in a system without clear priorities. By working together, collectively industry stakeholders can overcome siloes that hinder prevention.

The financial sector plays a critical role in fighting real-world criminals who devastate the lives of people in communities around the world with their heinous acts. Financial institutions are on the front line, rooting criminals out of the financial system — but they can't do it alone. There is a clear opportunity for the public and private sector to work together and align on a framework with defined measures of effectiveness for anti-money laundering and fraud detection efforts. A well-coordinated effort across regulatory agencies, financial institutions, law enforcement, and solutions providers is needed to make progress in achieving our goal of securing the integrity of the world's financial system.

"In that moment after the scam, I needed something to remind me I was human... not judgement and anger and fear."

- Lilah Jones, Business Email Compromise Survivor

"We are human beings. And this is a humanitarian crisis that we are living right now."

- Timea Nagy, Human Trafficking Activist & Survivor

References & Footnotes

[1] Values in this report are in U.S. currency, and are projections for 2023 unless specified otherwise.

[2] Banks ranged from $10 billion to over $500 billion in assets. Non-bank institutions had revenue ranging from $100 million to $5 billion.

[3] Verafin, *Insights from Five Related U.S. Criminal Court Cases,* March 2022

[4] Europe, the Middle East, and Africa

[5] Verafin, *Banking on Deceit: Billions Lost to Cybercrime & Authorized Push Payment Fraud,* 2023

[6] Verafin, *Business Email Compromise: Tracing the Lineage of a $50B Fraud Problem,* 2023

[7] Based on proprietary Nasdaq Verafin Cloud data analyzed in Q4 2023. For published results, visit *https://verafin.com/cloud-insights/*

[8] Verafin, *Understanding Fraud Schemes & Scams,* 2022

[9] The Department of the Treasury, *National Money Laundering Risk Assessment,* 2022

[10] White House, *A Proclamation on World Elder Abuse Awareness Day,* 2021

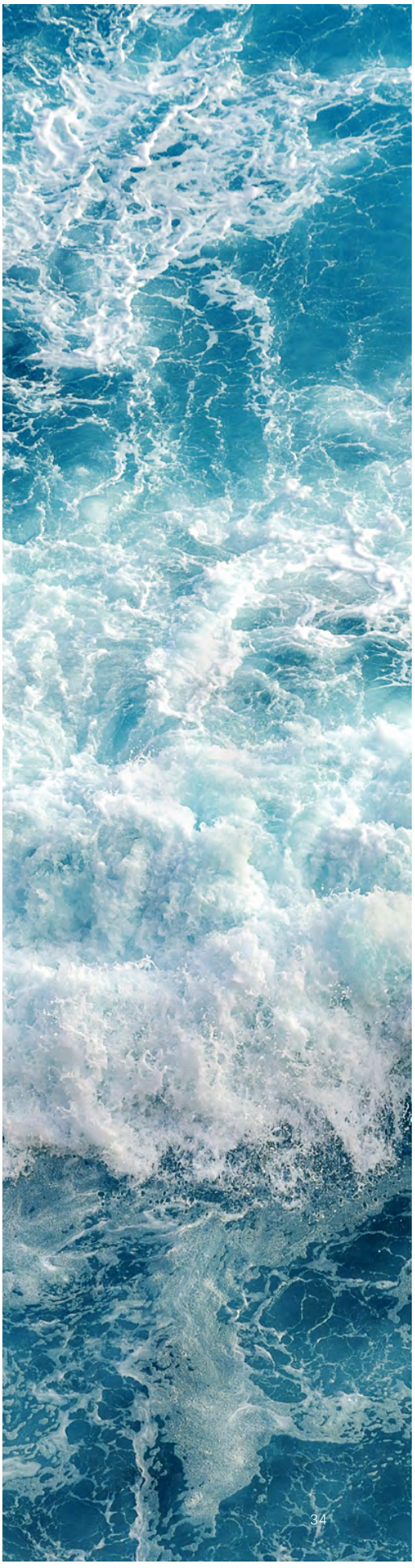
[11] Verafin, *Elder Financial Exploitation,* 2023

[12] Verafin, *Human Trafficking: Know the Behavior, Uncover the Crime,* 2023

[13] U.S. Department of State, *About Human Trafficking,* N.D.

[14] United Nations Office on Drugs & Crime, Global Report on Trafficking in Persons, 2022

[15] FINTRAC, *Operational Alert: Laundering of Proceeds from Online Child Sexual Exploitation,* 2020



Nasdaq (Nasdaq: NDAQ) is a leading global technology company serving corporate clients, investment managers, banks, brokers, and exchange operators as they navigate and interact with the global capital markets and the broader financial system. We aspire to deliver world-leading platforms that improve the liquidity, transparency, and integrity of the global economy. Our diverse offering of data, analytics, software, exchange capabilities, and client-centric services enables clients to optimize and execute their business vision with confidence.

To learn more about the company, technology solutions, and career opportunities, visit us on LinkedIn, on X @Nasdaq, or at www.nasdaq.com.

Verafin, a Nasdaq company, offers enterprise Financial Crime Management solutions, providing a cloud-based, secure software platform for Fraud Detection and Management, AML/CFT Compliance and Management, High-Risk Customer Management, Sanctions Screening and Management, and Information Sharing. More than 3800 financial institutions use Verafin to effectively fight financial crime and comply with AML/CFT regulations. Leveraging our unique consortium approach, Verafin significantly reduces false positive alerts, delivers context-rich insights, and more effectively fights financial crime.

To learn how Verafin can help your institution fight fraud, money laundering, and crimes such as terrorist financing, drug trafficking, human trafficking and elder financial exploitation, visit www.verafin.com, email info@verafin.com or call 866.781.8433.

Nasdaq VERAFIN A STEP AHEAD