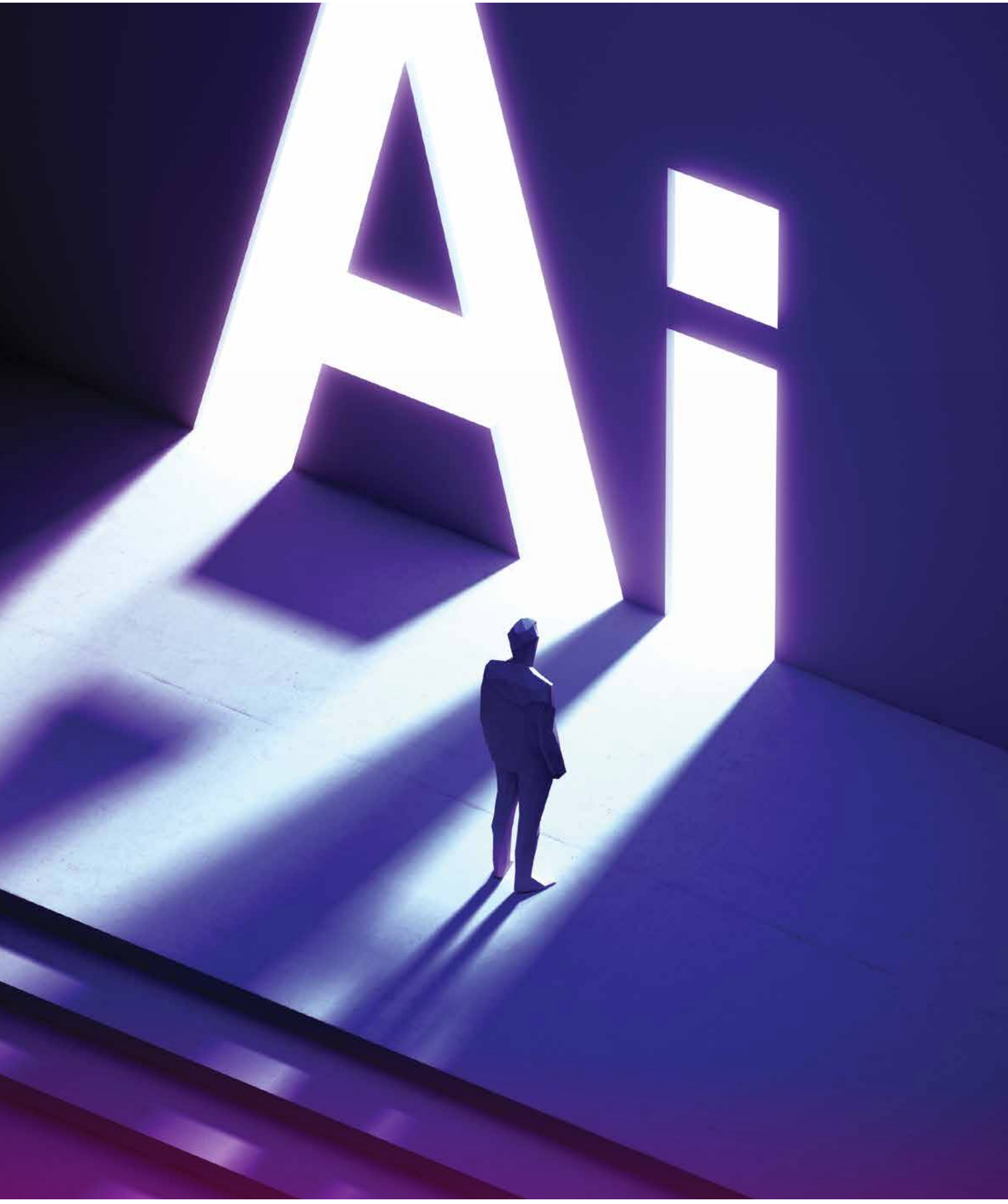
AI is poised to revolutionize accounting. But is the profession—and the humans in its ranks—ready for the sweeping changes to come?

Hard Reboot

By Andrew Raven



PHOTOGRAPH BY **ISTOCK**

On the surface, the headquarters of Stamped, a small accounting firm in Quebec City, looks fairly normal. The open-plan office space is sprinkled with hot desks, phone booths and meeting rooms. A few hanging plants provide a dash of green.

But Stamped is far from your typical accounting outfit. Alongside its tax and audit work, the company is developing an artificial intelligence (AI) system that founder Simon Langlois hopes will one day upend how accounting is done.

Although the technology is still in the testing phase, it can conduct background research on new clients, flag audit risks and generate planning documents, among other things. Long term, Langlois hopes it will take much of the grunt work out of auditing and free up accountants' time to concentrate on big-picture problems.

Langlois calls the system "Lucy" after the famous 3.2-million-year-old fossil of an *Australopithecus afarensis*—one of the first known primates to walk upright. "We're basically trying to create a new generation of auditors," says Langlois, a CPA and former manager at PwC Canada.

He's one of a growing number of accountants who have embraced AI, which experts say has the potential to revolutionize the accounting profession. The technology, its backers believe, could supercharge everything from forecasting to financial reporting to fraud detection. Many even see it as vital to the future of an industry struggling to attract new talent.

However, the rise of AI has raised some thorny questions for the profession. Among them: How do you make sure that AI is accurate? How much free rein should the technology be given? And, perhaps most importantly, in an era of superintelligent machines, what role do accountants have? Regardless of the answers to those questions, there's no putting the AI genie back in the bottle.

"I think it's our future. I don't think it's going away," says Cathy Cobey, the global responsible AI leader for assurance at EY and an accounting technology expert who co-authored three recent papers on AI for CPA Canada. Her message to those in the field? "It's still very early days, so this is a good time to experiment with it."

Accelerating change

For years, artificial intelligence has been used to reconcile bank statements, speed up data entry and categorize expenses, quietly streamlining how accounting is done. But the technology got a shot of adrenalin with the public release of OpenAI's ChatGPT in November 2022. What separated this so-called generative AI system from its forebearers was its ability to create human-like content from a simple word prompt. Suddenly, users could churn out everything from emails to *Twilight* fan fiction with a few keystrokes.

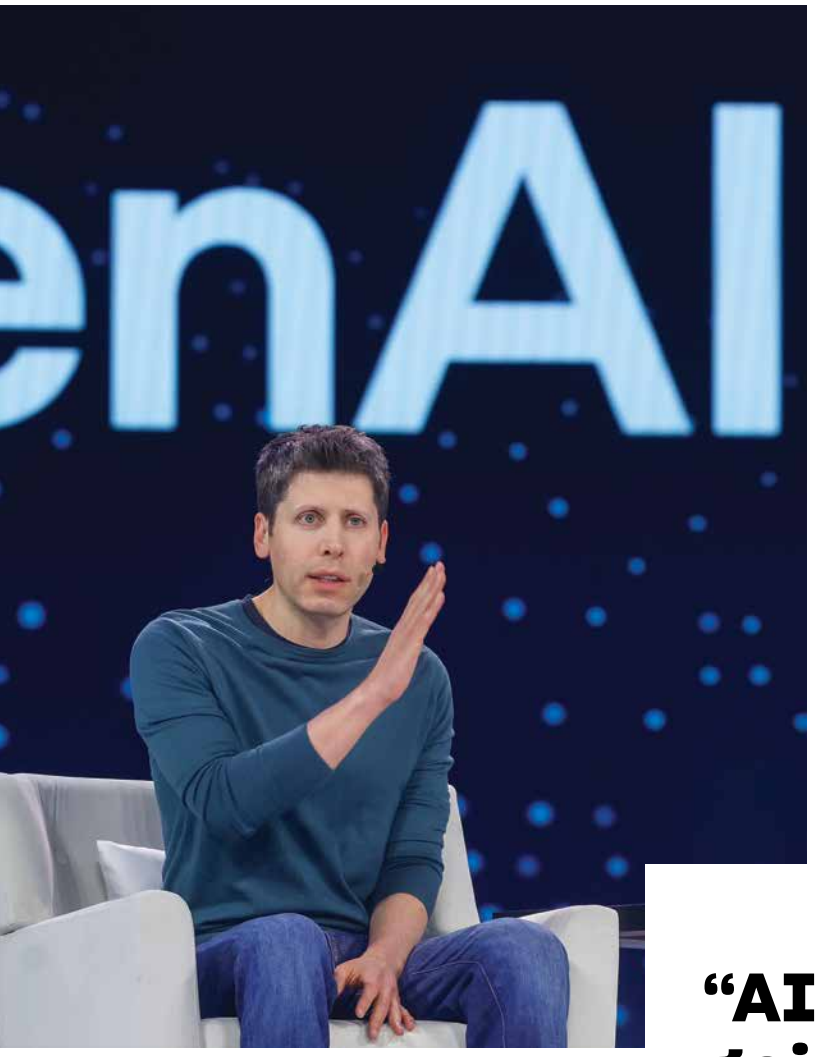
▲ OpenAI's Sam Altman speaking at the Snowflake Summit in San Francisco, California

PHOTOGRAPH BY GETTY

"I always thought that the AI market would be a hockey stick. It would be a really slow progression, but then something would [shoot] us up on the stick," says Cobey. "To me, that's what generative AI was."

It quickly became apparent that the technology could do more than tell bawdy tales of vampires and werewolves. Students began to use it to write term papers; web developers turned to it for coding; lawyers wielded it to draft legal arguments, sometimes to disastrous effect.

Accountants started testing it out too. Malik Datardina, a CPA and adjunct accounting professor at the University of Waterloo, remembers the first



time he tried ChatGPT. Shortly after its release, he quizzed the program on the finer points of auditing. The answer: a 10/10, says Datardina, an expert in accounting technology. "It blew me away. It was still audit-nerd speak but it understood [the theory]."

Three years later, use cases for AI have come into focus. Experts say the technology could one day generate detailed budget forecasts, create cash flow projections, develop risk-management reports, compile financial statements and analyze complex regulatory documents, including whether they apply to an organization. There's even a sci-fi-sounding future where AI-enabled drones handle inventory checks and AI-powered software ferrets out fraud by combing through millions of journal entries.

The result of that innovation, experts say, could be a revolution in financial and operational analysis—a new age of accounting where CPAs can probe deeper and forecast better than ever before.

An age of automation

Today, the use of AI in accounting is still very much in its infancy. Several large accounting firms, like EY, Deloitte, KPMG and PwC, are developing proprietary AI systems, many of which use ChatGPT and other open-source generative AI systems as a starting point.

At the same time, software companies like Intuit and Microsoft are rolling out AI-based features into their accounting programs, and a new crop of software developers are emerging, promising systems that can ease the burden on accountants.

Many of those solutions aren't ready for prime time. One of the papers Cobey co-authored cites recent data from Google that says even the largest language models—a subset of generative AI that powers ChatGPT—can still struggle with certain multi-step reasoning tasks, such as math word problems and common-sense reasoning. Some suffer from biases coded into their programming. Many are prone to making things up, a habit known as hallucination.

Those are all problems Sunith Varkey has experienced. He's a partner at Toronto-based One Accounting, a 20-person firm that specializes in bookkeeping and taxation. He's experimented with a start-up's AI-based receipt tracking program,

"AI is a tool that's going to make accountants more productive. We need to embrace and evolve with it. If we resist it, we are going to be left behind."

but it was error-prone. He tried using ChatGPT to code transactions, but it struggled.

Then there were the hallucinations. Varkey remembers asking ChatGPT if a non-profit could recoup land-transfer tax. It said yes. The answer, he later learned, was an unequivocal no. "We can't rely [on AI] in front of clients. We don't trust it," says Varkey, who uses ChatGPT and Google's Gemini largely to compose emails. But he views AI's problems as hiccups and is a big believer in the technology. "It's a tool that's going to make accountants more productive," he says. "I think we need to embrace and evolve with it. If we resist it, we are going to be left behind."

Many firms share that sentiment. More than eight in ten Canadian organizations are embedding AI into their financial operations, according to a January study from KPMG. Globally, KPMG expects 99 per cent of firms to be using AI for financial reporting within the next two years.

Security and accountability

The rise of AI is not without risks for a profession that at its core relies on accuracy and ethics. Langlois, the founder of Stamped, worries some accountants may rely too heavily on AI systems that haven't yet been perfected. He says some auditing firms facing debilitating staff shortages may be tempted to just run the AI and sign off at the end. "I think that's the risk that needs to be mitigated by CPA regulators," says Langlois. "How can we enforce corporate work ethic in the AI era, and [prevent people] from cutting corners at scale?"

AI systems are dotted with other potential pitfalls. Some platforms have suffered major data leaks and many leverage user information to train their AI, raising serious questions about data security. There are also concerns about who owns AI-generated content and whether that material sprang from copyright infringement. *The New York Times*, for example, is suing OpenAI, accusing the company of using its stories without permission to train its AI system.

Many believe the next step in the technology's evolution is agentic AI. Instead of simply offering a prediction or flagging problems, this new breed of AI will be able to make decisions and act on its own. A prime example: a system that can examine a purchase order, a goods receipt and an invoice, then make a payment.

Removing humans from the accounting loop will increase risk, but Cobey believes it's not an insurmountable problem. She says there are data science metrics that can be used to measure the accuracy and biases of AI outputs—similar to a heart-rate monitor for intelligent programming. "If you think about it, AI is really just math," says Cobey. "Math can be measured, tracked and compared against some type of tolerance band."

▲ Simon Langlois, CEO of Stamped, hopes the AI system his team is developing will one day upend how accounting is done

PHOTOGRAPH COURTESY OF **STAMPED**

To help address the concerns around AI, CPA Canada produced a series of three papers in 2024 and 2025. The reports explore the potential of AI-aided accounting, how companies can strengthen AI-related risk management and how AI might be used in assurance.

One of the key takeaways: as organizations barrel ahead with AI, they need to develop robust governance programs—ones that help ensure systems are trustworthy and aligned with societal, ethical and legal norms. That system, the papers argue, needs to parallel a commitment to oversight, including continuous checkups on how AI systems are working.

Mixed perspectives

AI has not yet risen to the level of an experienced accountant, but some worry it's getting close. In 2023, the program passed the CPA exam. Though, unlike the bar, it needed a second try. "We should all be proud," Cobey says, laughing.

For many, ChatGPT's success has raised a worrying question: Could AI one day make accountants obsolete? Some think a white-collar employment apocalypse is coming. Dario Amodei, CEO of AI developer Anthropic, told *Axios* that AI could wipe out half of all entry-level office jobs and drive unemployment in the United States as high as 20 per cent.

Others in the accounting world are less pessimistic. They predict AI will be more akin to productivity tools, like calculators or Excel. Cobey thinks machines could take over lower-level positions that focus on research, data entry and content generation. Experienced accountants will still be needed to wrestle with more complicated issues.

AI could also unlock a whole new set of jobs "that we don't envision today," Cobey says. "With every disruption, there are certainly some jobs that go away. But we always seem to create new jobs, create new complexity."

CPAs and finance professionals can have a role in making sure that AI investment decisions are based on high-quality data

That's a scenario Datardina could also see playing out. He compares the rise of AI to the advent of the automobile in the late 1800s. "If you grew up in a horse-and-buggy world and saw a car for the first time, you'd have no idea what kind of economic opportunities it would create," he says.

Datardina believes the future of white-collar professions, like accounting, will hinge on a larger public debate about the role of AI in society. Ultimately, he doesn't think tech companies or their government overseers have any interest in throwing millions of jobs into the wood chipper and unleashing Depression-era unemployment. "There's no money in losing jobs," he says. "If I get replaced by AI, then I'm not consuming. If you eliminate the consumer economy, you need a new economic system."

Ethical stewardship

Whatever the future holds, experts say CPAs shouldn't simply sit back and let AI wash over them. As stewards of financial integrity and overseers of control environments, they have a critical role to play in shepherding the rollout of AI across the business world.

CPA Canada's recent AI papers say that those in internal roles can shape AI governance and control. They can help their organizations validate the accuracy and completeness of AI-generated data, and guide how their employers spend money on AI.

"Executives are going to want to make sure that they're prioritizing their AI investments," says Cobey. "I think CPAs and finance professionals can have a role in making sure that those investment decisions are being made on high-quality data and include the full-cost accounting for the life cycle of AI."

Meanwhile, with mounting concerns over the reach and opacity of AI, industry players foresee a day when the technology will be scrutinized as closely as financial statements. That could unlock a whole new realm of assurance services as regulators, investors and others look for confirmation that businesses are using AI responsibly. CPAs can take the lead in developing the criteria against which AI systems will be measured or evaluated.

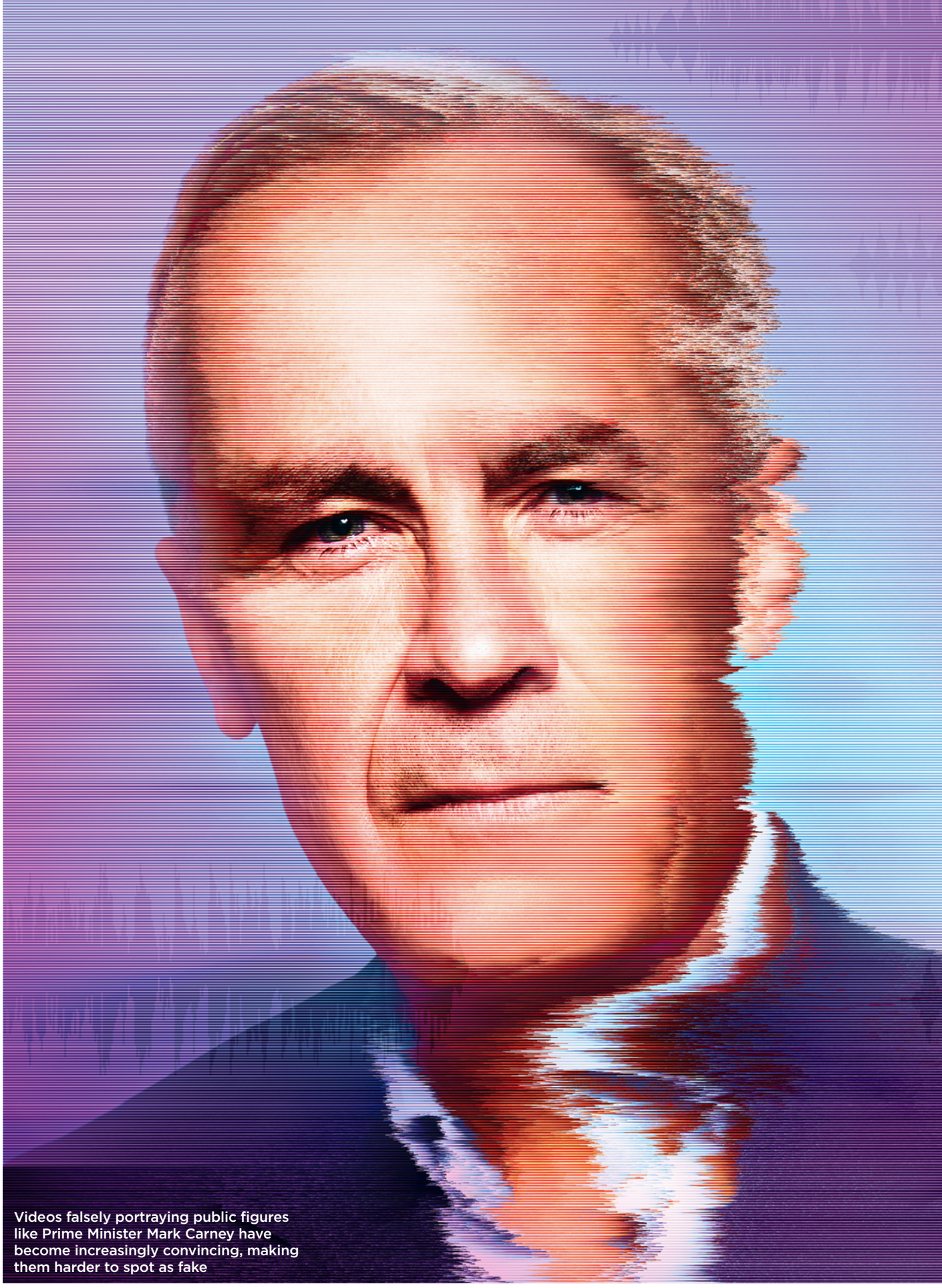
Looking forward

On Quebec's Magdalen Islands in the Gulf of St. Lawrence—a five-hour ferry ride from Prince Edward Island—Langlois, who works remotely, turns his computer camera toward the window. Visible is a treeless bluff and open ocean—fitting for a man who's made his living scanning horizons.

He and his team of roughly a dozen people are working on refining Stamped's AI system. Long term, they're hoping the technology will not only be able to flag risks but also act on them.

Langlois understands why many are worried about what AI means for accounting's future. In a world demanding ever more from the profession and accountants in increasingly short supply, modernizing is a must.

"We play a game where the rules are dictated by stakeholders," he says. "The biggest risk is that if the profession as a whole doesn't adopt new technology and elevate their games, the stakeholders may change the game." ◆



Videos falsely portraying public figures like Prime Minister Mark Carney have become increasingly convincing, making them harder to spot as fake

PHOTOGRAPH BY **RÉMI THÉRIAULT**

Look Again

The rapid spread of deepfakes has unnerved businesses and cybersecurity experts alike. As these AI-generated videos become more lifelike, CPAs will need to stand guard against the deception. **By John Lorinc**

Earlier this year, Instagram users with an interest in investing found a highly compelling post in their feeds: Abby Joseph Cohen, a legendary Goldman Sachs investment strategist who now teaches at Columbia Business School, popped up in a video, promoting three deeply undervalued stocks that, she seemed to be predicting, were set to experience enormous gains.

However, as a subsequent investigation by *Fortune Magazine* revealed and Goldman Sachs confirmed, the videos were "deepfakes," constructed by generative AI software using existing online video and audio clips of Joseph Cohen. *Fortune* found numerous examples of deep-faked investment execs starring in other social media pump-and-dump schemes. "AI-enhanced scams pose significant risks to investors," observes Bonnie Lysyk, former Ontario auditor general and currently the Ontario Securities Commission's (OSC) executive vice-president for enforcement. "The use of AI can divert those investors away from legitimate sites to fraudulent sites," she adds, citing research carried out by the OSC and other securities regulators.

Although deepfake technology is most closely associated with phony celebrity videos and AI-generated porn, there's a growing list of examples of the technology being used by international criminal organizations intent on defrauding corporations as well as gullible investors. Bad actors now equipped with inexpensive and easily accessed software tools have found novel ways to use deepfakes to mess with internal financial controls, hiring and onboarding systems, authentication protocols thought to be secure and a range of other systems.

Indeed, such uses of generative AI are proliferating rapidly, and now pose a daunting challenge to corporate cybersecurity teams and their advisers, who have spent years training managers, employees and executives to be aware of phishing schemes and ransomware attacks. Almost overnight, the list has grown to include the criminal use of deep-faked voice clips—a.k.a. spoofing—to gain access to consumer banking services. "Emerging technologies such as AI have a rapid development and deployment strategy," says Peter Hargitai, PwC Canada's national digital risk solutions leader. "Therefore, a disciplined and thoughtful approach is needed to timely embed cyber and data trust protocols and controls."

Trust under siege

Many of us have probably tried one, with mixed results: those news site quizzes that test your ability to distinguish a real image from an AI one. There are the most obvious clues—too many fingers, unnaturally smooth skin, missing shadows, etc.—but generative AI's ability to learn from its mistakes has meant that the clues have become ever more difficult to spot without sophisticated scanning tools.

Not surprisingly, a 2025 report by the Association of Certified Anti-Money Laundering Specialists ranked criminal use of AI as fourth of the ten most worrisome financial crime threats currently in circulation. "The use of generative AI for malicious purposes continues to profoundly reshape the threat environment," the authors wrote. "The sheer speed, scale and sophistication of criminal exploitation—notably with malware, social engineering and video/voice cloning, sometimes referred to as 'deepfakes'—make this one of the most significant threats to financial crime functions."

For CPAs providing guidance on risk, cybersecurity and data governance, the deepfake threats facing corporate clients are not just formidably fluid but potentially expensive. A frequently cited and bracing

Abby Joseph Cohen, former chief investment strategist at Goldman Sachs, was targeted in a deepfake stock scam ▼

Employees must know how to respond swiftly to AI-enabled deception before financial or reputational damage occurs

public example involves a Hong Kong–based finance worker with Arup, the U.K.-based engineering giant, who was summoned to a virtual meeting with other members of staff and told to transfer US$25 million to an external account. He followed the instructions. As it later transpired, the entire virtual meeting session had been convincingly manufactured by deepfake fraud artists. (Arup declined to comment.) "The incident speaks to how advanced the capabilities of these tools have become and continue to evolve," says Melissa Robertson, CPA Canada's principal for research and thought leadership. "It's getting much harder to be able to differentiate when it is an AI versus when it is a person."

"Generative AI tools are much more accessible to create convincing fraud," adds Alan Mak, BDO's national forensics practice leader. "The earlier phishing emails, in hindsight, were pretty easy to detect. You get an email that on the header says it came from our CEO and click onto it. It's pretty obvious that the actual email address is not the address; it's something else. Now we're talking about either audio or visual fakes, or both, that would be harder to detect because it looks like you're speaking to, or it feels like you're speaking to, the person you think you are. But in reality, you're not."

While incidents such as the one in Hong Kong get a lot of attention, voice "spoofing" is another pressing concern because so many companies, like banks and telcos, have adopted voice authentication to make it easier for customers to access their accounts remotely. This year, OpenAI announced its latest platform could create precise voice replicas based on just 15 seconds of authentic audio, a capability that effectively weaponizes the seemingly limitless amount of audio now available online, through social media, podcasting, YouTube and more. (Deepfake voice prints have been implicated in some notorious consumer frauds, such as the grandparent scam, where fraudsters place calls to elderly relatives asking them to immediately transfer large sums to deal with an emergency situation involving a beloved grandchild.)

Voice spoofing has rapidly upended what many cybersecurity experts regarded, until recently, as a robust verification tool. Customers could record themselves, and the algorithm was trained to recognize their voices when they called in to do their banking. That's not the case anymore. Earlier this year, *The Wall Street Journal* reported that Chase Bank's voice authentication system was "fooled" during a test, although the bank insisted it has other backup verification systems. According to a 2024 report by cybersecurity solutions provider BioCatch, over nine in ten banks are now thinking about eliminating the feature in favour of the most robust dual-factor authentication systems—a statistic in wide circulation. "If you reach out to the contact centre of some of your current service providers," says PwC's Hargitai, "and you've signed up for their voice authentication, you can practically go all the way through and start transacting. Appropriately protecting and safeguarding telephony technologies is a must."

As concerning are the use of deepfakes in cybersecurity fraud aimed at senior finance executives and repositories of valuable corporate data. A recent Deloitte survey found that over a quarter of respondents had been targeted by fraudsters looking to steal financial data within the last year. In other cases, deepfake technology is being used to create false online customer IDs using stolen, personally identifiable information (PII), as well as AI-generated photos imported to deep-faked documents, such as driver's licences and passports.

Recruitment processes, in turn, have become a particularly vulnerable portal because so much hiring and onboarding is now done virtually. "During COVID, we saw people pretend to be someone else to get a job, but they're really not that person and they're not even qualified," says Marilyn Abate, a partner in KPMG's Toronto forensics team. "With deepfakes, they can make it look like [someone else]. And if they're working remotely all the time, you'll never know who the real person is." The payoff for the fraudsters, she says, is access to the company's

PHOTOGRAPH BY GETTY

internal systems. "Sometimes the criminals will plant people in organizations to commit insider fraud."

One U.S. cybersecurity service provider recently posted a story about how, when seeking to fill a routine IT position, it inadvertently hired a North Korean programmer looking to infiltrate the organization; the individual was using a stolen U.S. ID that had been enhanced with AI, but eventually left a trail of increasingly suspicious digital bread crumbs. In other cases, fraud artists posing as executive recruiters for well-known firms will lure job seekers through networks like LinkedIn, then demand applicants pay a fee to continue the process. As Abate adds, "I've seen examples of larger organizations that's happened to—that [fraudsters] infiltrated the organization through this technique and were able to commit fraud, steal money and do other bad things."

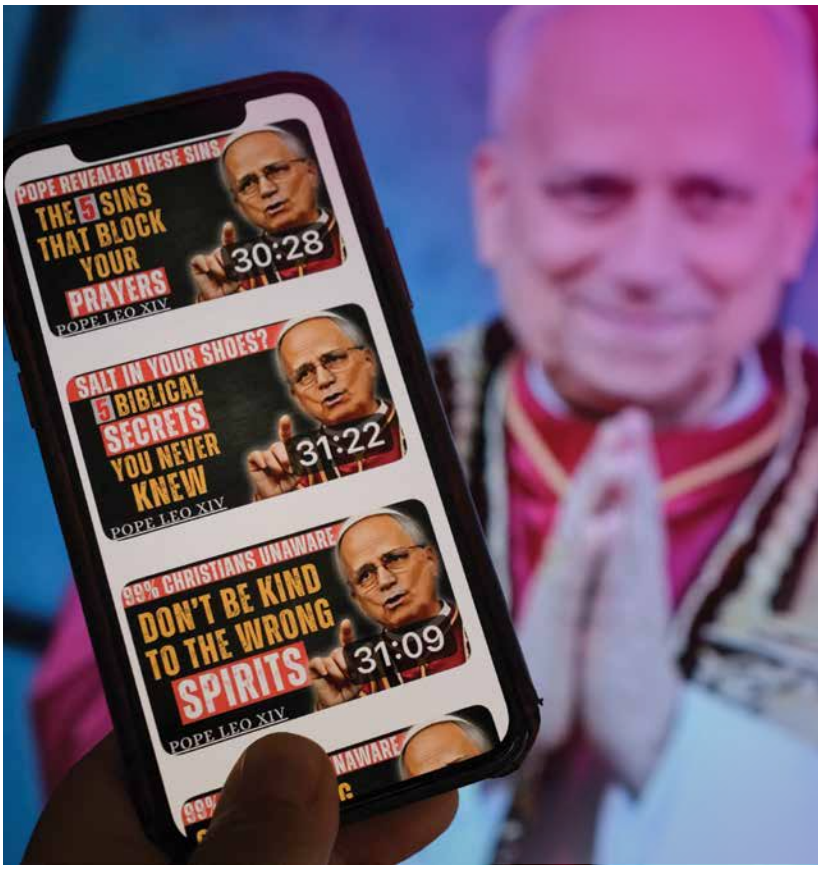
International responses

Given a technology as dynamic as generative AI and a globalized threat environment, regulators and enforcement agencies have found themselves playing catch-up, as usual, but there's evidence that most are trying to respond in real time.

In late 2024, the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) released a detailed alert to advise financial institutions on how to detect the types of deepfake threats that should be included in suspicious activity reports collected under banking legislation.

The document not only detailed recent developments in generative AI but itemized numerous reported techniques used by criminals to create customer accounts with fake documents made via deepfake technology or the use of deepfake audio/video in phishing emails. FinCEN's guidance included a list of nine red flags and related clues, such as inconsistency between customer documents, the use of third-party webcams during video authentication calls and, of course, suspicious patterns of account activity. Among its list of best practices: live verification checks initiated by the financial institution in which the customer is prompted to confirm their identity using video or audio.

Here, the Canadian Securities Administrators' network of provincial regulators, as well as the Office of the Superintendent of Financial Institutions (OSFI) and the Canadian Centre for Cyber Security, have all issued similar warnings to market participants, issuers and investors. In a recently published alert, OSFI and the Financial Consumer Agency of Canada also listed the types of threats posed by generative AI, including incursions aimed at smaller banks and credit unions, which traditionally avoided attacks because their size makes them less attractive to criminal gangs.



▲ AI-generated videos of Pope Leo XIV are spreading online fast, racking up views as platforms struggle to rein them in

"Between the securities commissions and the other regulators in Canada and the investment players, I think there's work being done to try and address the problems that we're seeing with impersonation," says Lysyk. Yet Hargitai argues that rules governing corporate disclosure to capital markets for AI-related cybersecurity risk mitigation and related governance activity are still evolving in Canada, and more is needed to address the evolving risk vectors.

The enforcement end of the story is even less encouraging. Last year, the European Union, which takes a proactive approach to data protection, passed the AI Act. It includes provisions requiring developers and deployers to reveal to end users when they're interacting with AI (for example, via chatbots or deepfakes), according to an extensive summary by University of British Columbia law professor Benjamin Perrin. He also points to the first Canadian court case involving deepfakes of child sexual exploitation, based on charges brought against a 61-year-old man who not only collected online child porn, but pleaded guilty to creating at least seven videos with so-called deepfake technology.

PHOTOGRAPH BY GETTY

"The rise of increasingly genuine-looking audio and visual deepfakes, now powered by AI, has added one more tool to the arsenal of threat actors"

As for deepfakes used in fraud or cyberattacks on companies, Canada doesn't have much in the way of significant legal protections, says Lisa R. Lifshitz, a Torkin Manes partner who chairs the firm's technology, privacy and data management practice. "We don't actually have bespoke deepfake legislation," she says, describing the unnerving experience of watching presenters at tech law conferences produce highly convincing deepfakes in minutes. "We have certain federal laws, such as the Criminal Code, that prohibit fraud, identify theft and harassment, for example, and copyright laws that offer certain protections, but we don't have deepfake legislation," says Lifshitz.

She noted that existing Canadian privacy laws offer limited recourse if the deepfakes do not reveal personal information. Certain provinces have recognized the statutory tort of unauthorized use of someone's likeness and the tort of "appropriation of personality." The tort of "false light" has been upheld in Ontario, but Lifshitz adds that financial penalties are so low that they provide little protection.

Another potential cause of action is defamation. The Quebec Civil Code confirms that individuals have a right to the respect of their reputations and privacy, and a deepfake that appropriates or uses a person's name, image, likeness or voice for a purpose other than the legitimate information of the public would be a violation under the code.

Lifshitz and other experts note that problems or frauds associated with deepfakes must become a routine part of what corporate cybersecurity teams monitor, in terms of identification, technology defences, data governance, training and other forms of risk mitigation. "Unfortunately, the rise of increasingly genuine-looking audio and visual deepfakes, now powered by AI technologies, has added one more tool to the arsenal of threat actors that require constant vigilance," she says. The wrinkle, adds Mak of BDO, is that the technology "enables bad actors to bypass some of our traditional controls."

In some cases, the prevention and risk-mitigation tools are actually embedded in classic approaches to financial governance. The notorious case of the Arup manager in Hong Kong revealed a weakness in the company's internal systems, says Robertson of CPA Canada. "One individual should not be able to go start to finish to transfer $25 million." The incident, she adds, "emphasizes the need to have proper internal controls in place so that you can prevent situations like that from happening."

In some cases, says Abate of KPMG, executives and managers have begun to use an additional level of authentication, such as a "safe word" that can be used when someone posing as a company official has directed another employee to make a large transfer. "It's something that only you and I know so somebody else can't mimic it," she says.

The turbocharged sophistication of deepfakes has also made regular cybersecurity training that much more important. To some extent, Mak acknowledges, it's always going to be a matter of playing catch-up. "Our clients are running fraud training and phishing training two, three, four times a year, which means there could be anywhere from three months' to twelve months' delay in employees or staff hearing about what's happening, whereas the bad guys are constantly evolving." Best practice involves follow-up tests and consequences for those who repeatedly fail.

"Having the right level of investment in this area," adds Hargitai, "is going to be an ongoing battle." The tool kit includes security-by-design approaches to IT systems, such as minimizing the number of people with access to PII or customer accounts. Another risk-mitigation tool involves technologies that can screen for voice spoofing or add digital watermarks to authentic video, flag deepfakes on platforms like Zoom or check the source of a video feed to see if it traces to a known address. Yet an evaluation of AI uses in capital markets, published

this year by the International Organization of Securities Commissions, warned that these techniques are "not comprehensive and can be evaded."

Opinion on the efficacy of such tools remains mixed. "They can be effective," says Mak. "My caution is that you should not rely on them 100 per cent for obvious reasons. They provide a good first line of defence, but my advice is generally to use multiple lines of defence." Lifshitz is more skeptical: "Using digital watermarks may be helpful now, but in the longer term, AI technology will make them obsolete."

Because the technical sophistication means deepfakes are much harder to detect, Abate stresses that employees in large organizations shouldn't necessarily be trying to decode a suspect image themselves; all they need to do is be alert to something that doesn't seem quite right. "That's why you need the training because they can't just rely on the system," she says. "You need people's eyes. You don't have to train [employees and managers] to know what to do with [a suspect deepfake]. Just raise your hand and tell someone."

The last move involves incident response tailored to the deepfake threat in particular, as one cybersecurity expert told a U.S. Securities and Exchange Commission investor forum this year. "The rise of AI-driven scams means businesses must be prepared for deepfake-enabled fraud, synthetic identity attacks and AI-enhanced phishing schemes," said Perry Carpenter, a deepfake researcher. "Organizations should update incident response plans to include rapid fraud assessment procedures, forensic AI analysis capabilities and clear internal escalation paths. Employees, finance teams and security personnel must know how to… respond swiftly to AI-enabled deception before financial or reputational damage occurs."

Future certainties

Two things are clear in this volatile domain: one, that deepfakes and their uses will become inexorably more realistic, persuasive, numerous and therefore difficult to identify; and two, that the rise of this brand of cyber threat will produce lucrative new business lines for cybersecurity consultants and other advisers. Deloitte's Center for Financial Services estimated last year that GenAI could enable fraud losses to reach US$40 billion in the United States by 2027, so firms need to invest in prevention, training and detection or they'll face bracing losses associated with the mischief that deepfakes can inflict. "Unfortunately," Mak muses, "people don't really take it seriously until they've been hit. But once they've been hit, everyone takes it very seriously." ◆

DIGITAL IMPOSTORS

How deepfakes can slip into financial services

By John Lorinc

Last year, the Financial Services Information Sharing and Analysis Center, a Virginia-based cybersecurity not-for-profit, published a list of scenarios of existing deepfake scams that pose a risk to the financial industries. These include:

C-suite impersonations targeted at investors, employees or consumers in the service of pump-and-dump schemes, fraud and access to personally identifiable information

Scams that leverage voice print identification to bypass banks' customer verification controls, gaining access to consumers' accounts to defraud them

Deepfake videos that replicate financial advisers or investment bankers' likenesses, using their identities and reputations to commit fraud or other forms of online misrepresentation

Deepfakes that impersonate third-party advisers who have relationships with financial service firms, which can then be used to gain access to or exfiltrate money from these firms

PHOTOGRAPH BY ISTOCK

Secure Browsing

A close look at the WebTrust for CA audit program that keeps Certificate Authorities accountable—and the Internet safer for everyone

By Stephanie Matas

ILLUSTRATION BY **ISTOCK**

In a world of rising cyber threats and digital misinformation, knowing who to trust online is more important than ever. Behind the scenes, a system of checks and balances helps keep the Internet secure, and at its heart is the WebTrust for Certification Authorities (CA) program.

The WebTrust for CA program was developed from 1999 to 2000, as part of the initial WebTrust program by the AICPA and then CICA in 1997. This audit program aims to increase consumer confidence in the Internet, providing a framework for evaluating if businesses operating online meet requirements of security, identity verification, compliance, and certificate and key life-cycle management.

Today, WebTrust for CA is managed by CPA Canada and continues to provide greater trust and accountability in the digital sphere by examining CA's controls and practices to ensure they meet established criteria based on externally accepted control standards for public key infrastructure (PKI).

Guardians of digital validation

A CA is a trusted entity that validates the identities of websites, email addresses, companies or individuals, and binds them to cryptographic keys through the issuance of digital certificates. Essentially, they act as a trusted third-party in online transactions, ensuring that the platform users are interacting with is the one it claims to be.

PKI represents the system of digital certificates, policies and procedures needed to ensure secure communication between web browsers and servers. It uses public-private key pairs, which have a unique mathematical relationship. An encrypted message with a public key can be decrypted only with the private key, and vice versa—a message signed with a private key can be verified with a public key.

How it works: A subscriber, which is a CA's customer, obtains a public-private key pair, generated manually or using an automated certificate management system. Once the pair is generated, the public key is held by the user and on a remote server. The subscriber then goes through a registration process by submitting their public key to a CA or registration authority (RA) acting as an agent for a CA. The CA or RA verifies the identity of the subscriber according to the CA's established practices, then issues a digital certificate.

The CA will manage the digital certificate throughout its lifecycle, from registration to expiration. They are also responsible for providing certificate status information. However, CAs can be constrained and restricted in a variety of ways. For example, a CA may be limited in the types of certificates it can issue based on where it sits in the hierarchy.

Root CAs are the highest authority, which are trust anchors usually kept offline. They sign the certificates of intermediate CAs, establishing the base level of trust. Intermediate CAs operate under the trust of a Root CA, issuing certificates to end-entities like websites. Below them are subordinate CAs, which issue certificates on behalf of the Root CA, allowing organizations to have their own internal CA.

Trust starts here

The main mission of the WebTrust for CA Task Force is to design and maintain an audit and compliance program that supports the needs of the PKI community and builds trust throughout the ecosystem, says Tim Crawford, principal and WebTrust for CA practice leader for BDO USA and co-chair of the WebTrust Task Force.

The task force introduced the first draft of criteria and principles for WebTrust for CA in August 2000, says Don Sheehy, one of the original members and WebTrust Task Force chair for over 10 years. With the assistance of the American Bar Association, it translated technical standards of ISO 21188, which provides directives for managing PKI in the financial services industry, into auditable criteria.

Sheehy says the growth of electronic commerce in the '90s created security and privacy concerns. "There was a projection that e-commerce was going to continue to grow exponentially. When the growth pattern appeared to begin to flatten due to concerns, PKI was recognized as a solution. A number of big players thought PKI was going to be the next big thing, so our task force jumped on it."

Although there are many types of WebTrust engagements, WebTrust for CA is the main audit that all CAs seeking public trust must undergo annually. It assesses the adequacy and effectiveness of controls by a CA. Core components include:

- **Business practices and disclosure compliance** The CA's Certificate Policy (CP) and Certification Practices Statement (CPS) must be made available to all relying parties (most are typically published on the CA's website). Auditors verify if the illustrative controls in the WebTrust framework align with what the client has stated, says Chris Czajczyc, Deloitte's global representative on the WebTrust Task Force.

- **Subscriber identity verification**
  Each certificate request is checked to ensure the subscriber's identity is valid (such as organization name, domain name, device characteristics). For example, to prove that you are in control of a given email address, they may send you a message and you have to reply back with a certain response to indicate that you control that email address. Auditors look for robust subscriber registration and verification processes, including the training of personnel and the strength of built-in controls, says Czajczyc.

- **Cryptographic key and certificate management**
  Auditors test technical and process controls over cryptographic keys and certificates. This includes secure key generation, storage, backup/archival, use and destruction; proper issuance and renewal of certificates; and timely revocation, if needed. The audit checks that private keys remain confidential and that certificates are signed and released only under the prescribed conditions, with "auditors and relying parties focusing on the CA's ability to quickly detect errors, revoke incorrect certificates and issue proper ones," says Czajczyc. "The ecosystem demands swift reactions to mistakes, as failure to do so can lead to distrust, severe business implications and even the downfall of CAs."

  CAs also have to constantly provide a status report notifying a relying party if a certificate is valid. If it expires or is revoked, the status will be updated. A certificate might be revoked if a company experiences a cyber breach and its web server is compromised or if they are involved in an acquisition and there's a change in website or company name. "A CA is responsible for providing certificate status information 24/7, and a popular website might generate millions of requests a day to determine if a certificate is still valid," Crawford says.

- **System and data security**
  The CA's IT environment must be securely configured and monitored. Auditors review general IT security practices, including logical and physical access controls, risk assessments, vulnerability scans, data retention policies and confidentiality measures. Czajczyc stresses that auditors need extensive technical expertise and professional judgment to assess compliance in complex environments.

Major players in the WebTrust ecosystem

- CPA Canada is responsible for approving, maintaining and publishing WebTrust principles and criteria for various assurance domains, as well as providing practical guidance and illustrative assurance report samples for enrolled practitioners. It handles enrolment of public accounting firms and practitioners to conduct WebTrust engagements, and oversees and supports the WebTrust Task Force. It also authorizes and manages the issuance of the WebTrust marks (seals) through its WebTrust Seal Program and defines how both practitioners and their clients may use and display them. Collaborating with various WebTrust program stakeholders, CPA Canada makes sure evolving CA/Browser Forum requirements and market demands are reflected in the WebTrust program too.

  "CPA Canada serves as the oversight body within the WebTrust ecosystem, enrolling practitioners, overseeing the WebTrust Task Force and having the final say on updates to the WebTrust program's principles and criteria," says Lilia Dubko, senior manager, assurance programs for CPA Canada, and WebTrust Task Force co-chair

- The WebTrust Task Force is the backbone of the program, composed of public key infrastructure (PKI) and assurance experts. They develop the WebTrust principles and criteria used to perform WebTrust audits, and update them periodically based on insights from the CA/Browser Forum and Authindicators Working Group. It's also charged with developing assurance engagement reporting templates, providing guidance to practitioners, supporting the browser community regarding root programs, and helping guide the future of online assurance.

  "By supporting the WebTrust Task Force, we bring together practitioners who develop the engagement criteria that are relevant and evolve with the users' needs," says Taryn Abate, director of research and thought leadership for CPA Canada

- Indirectly involved is the CA/Browser Forum—a voluntary group of CAs, browser software vendors and suppliers of other applications that use digital certificates—which defines the baseline standards for the CA industry. Any forum member can propose changes or additions to requirements by outlining the proposed change, the problem it addresses and how to solve it, then submitting it as a ballot to be voted on. CPA Canada proudly hosted the CA/Browser Forum in June.

  "By having a presence at the CA/Browser Forum and engaging the browsers throughout the year, we hear their views on the assurance engagements being performed today as well as potential needs for the future," says Abate.

- The Authindicators Working Group, a band of industry experts who develop technical specs for Brand Indicators for Message Identification (BIMI), is also indirectly involved. BIMI is a fairly new technology that allows organizations to use their logo to verify emails, which relies on digital certificates issued by CAs to authenticate the sender.

How a WebTrust for CA audit works

1. An auditor helps the CA select the audit criteria for the scope of the engagement. This involves "understanding the scope of the systems and services, planning out where we need to visit, who we need to talk to and what kind of evidence we need to get," says Crawford.

2. The auditor tests the CA to determine whether it meets the required disclosure, integrity and security requirements. "We test a wide range of manual and automated controls, such as door locks, storing assets securely, taking inventory of assets, managing access and automated validations of identity," says Crawford. Auditors look to determine if CAs have good procedures for onboarding employees, validating client identities and whether changes are done in a secure manner, involving risk assessments and testing processes.

3. An assessment is made, and if there's no significant deficiency that year, the CA receives an unqualified or clean audit report. "An unqualified opinion means we agree with management's assertion that they've met all the criteria in their policy and procedures in accordance with the WebTrust framework," says Crawford.

   On the flip side, a qualified report means there are areas where controls failed to address the criteria. Some examples of common control failures are delayed revocation (public CAs are required to revoke certificates within 24 hours) or the certificate does not contain information required in the templates.

4. Once a clean, unqualified audit report is established, it's reviewed and approved by management and then submitted to CPA Canada, which reviews the report for accuracy. Though qualified audit reports don't require submission to CPA Canada, browsers recommend obtaining a seal to prove the legitimacy of all reports.

5. Upon acceptance, CPA Canada will issue a WebTrust seal, indicating that the CA has been independently audited and found to be in compliance with WebTrust principles and criteria. The seal can then be displayed on a webpage. If a user clicks on the seal, they'll be redirected to a page that displays the audit report.

25

The number of years WebTrust has bolstered confidence and trust in online security

Integration with browsers

One of the major reasons for the success of WebTrust for CA was the creation of the Microsoft Root Program in the late 2000s. Today, it has become an integral part of trusted root programs for other major browsers, such as Google, Mozilla and Apple. Root programs are systems that maintain a list of trusted CAs whose digital certificates are considered valid and safe to use by operating systems and applications.

A WebTrust seal shows root programs that the CA passed its audit and is trusted enough to be included in their list of approved root certificates, which come pre-installed in browsers and operating systems. Inclusion in this root store demonstrates a chain of trust, so a browser will display the site as secure. If a website's certificate is not trusted, a browser may display warnings or error messages, which in turn can prevent users from accessing the site.

A CA's own claims of compliance carry limited credibility. Browsers rely on the independent, objective audit processes, evidenced by the WebTrust seal, to be included in their root stores, says Ben Wilson, CA program manager at Mozilla. The reliance on WebTrust auditors is based on their adherence to a code of ethics and professional standards, ensuring independence from the CA being audited, says Wilson. "Whenever I take an action, in respect to looking at a CA and the WebTrust report, I have to ask myself, 'How do the CA operations affect my end users in terms of their privacy and their security?'" Mozilla prioritizes CAs for root inclusion based on their compliance history and audit results, as well as the financial capability to support the full range of compliance obligations—including retaining qualified personnel, maintaining secure and trustworthy infrastructure, and obtaining required independent audits such as WebTrust, he says.

Looking ahead

While there is competition with the European ETSI program, WebTrust remains the only program in North America that meets the required audit standards for public acceptance.

With the future of digital services ever-expanding, Sheehy says the challenge now is adapting audits to new delivery models like cloud services and distributed processing. He hopes for better alignment with current international standards like ISO 21188 and 27099, and increased global promotion to counter competition from ETSI.

Czajczyc says that, although WebTrust for CA has Canadian and U.S. roots, it's a global program. Developments in the WebTrust ecosystem are happening worldwide, particularly in Asia, Europe

and Africa, reinforcing the need for global co-operation to ensure the program remains relevant and responsive. "If we use the moment of opportunity that we have now to transform, as connectivity, smart cities, smart infrastructure, critical infrastructure grows—all of it needs to be trusted," says Czajczyc. "Without a program in place to ensure better trustworthiness, it's going to be a scary world out there."

Under the guidance of the WebTrust Task Force and with insights from the CA/Browser Forum, WebTrust for CA will continue to evolve and adapt to new and emerging technologies—for example, document signing, digital identities, the Internet of Things (IoT), digital wallets and autonomous vehicle technology. But right now, only a small portion of the PKI use cases are being audited. Moving forward, the WebTrust Task Force is looking to expand the program and bring more structure to the ecosystem.

Connection to CPAs

For CPAs, WebTrust for CA represents more than just a technical audit; it enhances their professional credibility, opens doors to new client services and builds trust in digital systems. "The standing of CPAs, their trustworthiness and professional credibility within the assurance world directly support trust in the global Internet security infrastructure," Dubko says.

By stepping into this specialized area of IT and cybersecurity, CPAs bring real value to businesses, governments and the public, helping ensure that secure communications remain trustworthy and reliable. WebTrust for CA relies heavily on the qualifications, ethical standards and auditing expertise of CPAs to deliver meaningful, independent third-party assurance. Czajczyc says that CPAs, especially those with backgrounds more broad than just financial auditing, are essential for issuing trusted WebTrust reports. The rigorous requirements and governance of the CPA profession provide value and credibility in WebTrust engagements.

"CPA Canada manages this program because we believe in the vital role the accounting profession plays in sustaining confidence in information security," says Abate. "This is a global program and we are proud to support the standardization of these offerings across jurisdictions to keep the assurance results comparable and credible worldwide."

The future is bright for this globally recognized program, now celebrating 25 years of success. By working closely with the leaders who set and uphold PKI standards, and with CPA Canada's oversight, WebTrust for CA will continue to evolve and thrive. Combined with the dedication of key volunteers and the flexibility to tackle emerging cybersecurity challenges, its impact will only grow stronger. ◆

"The WebTrust for CA program relies heavily on the professional qualifications, ethical standards and auditing expertise of CPAs to deliver meaningful, independent third-party assurance. The value and credibility of WebTrust reports stem directly from the rigorous framework governing the CPA profession."

—Lilia Dubko, senior manager, assurance programs for CPA Canada, and WebTrust Task Force co-chair

Integrity pillars

These key elements define a CPA's role in WebTrust.

- **Independence and objectivity.** CPAs are independent from the entities being audited, which ensures WebTrust audit reports are unbiased, conflict-free and can be trusted by browsers, regulators and users.
- **Ethical and professional conduct standards.** CPAs adhere to a strict code of ethics surrounding integrity, objectivity, professional competence, confidentiality and due diligence, which are crucial when evaluating complex technical environments like PKI.
- **Expertise in assurance services.** CPAs are trained to attest and provide assurance services under AICPA's Statements on Standards for Attestation Engagements (SSAEs), Canadian Standards on Assurance Engagements (CSAE) 3000-3001 and/or International Standard on Assurance Engagements (ISAE) 3000, enabling them to assess in a systematic, evidence-based manner.
- **Standardized methodology and documentation.** WebTrust engagements follow a structured methodology. As CPAs are trained to document their work in a way that supports transparency, quality control and peer review, they ensure audit results are reliable and comparable across CAs and jurisdictions.
- **Peer review and quality assurance.** Firms performing WebTrust audits must undergo periodic peer reviews, underscoring the critical role of CPAs in upholding professional standards, high-quality practice and the credibility of these audits.
- **Recognition by browsers and root programs.** Major browser vendors require WebTrust for CA audit reports to be conducted by qualified CPAs (or equivalent), relying on the profession's trustworthiness to decide whether a CA can remain in a trusted root store.

ILLUSTRATION BY ISTOCK