CELLTRUST®
SECURE & COMPLIANT MOBILE

Why are secure and compliant enterprise level mobile business communications solutions critical for financial services?

“CellTrust was founded in 2006, with the vision that the mobile device would become crucial to validating identity and the trusted and convenient exchange of relevant, confidential, enterprise or personal data. Within a little over a decade, our vision became a reality. The mobile device has become the authentication channel of choice for most individuals, governments, and enterprises worldwide.” — Sean Moshir, Co-founder and CEO.

The CellTrust secure and compliant mobile communication platform is engineered by the pioneers of anti-virus software and the multi-billion dollar enterprise patch management industry, which now secures over 90% of IT systems around the world

Our vision became reality

CellTrust was founded in 2006 with the vision that the mobile device would become crucial to validating identity and the trusted and convenient exchange of relevant, confidential, enterprise or personal data.

In the past, within our ebooks, we used to spend quite a bit of effort convincing decision makers why a mobile-first communication strategy was important for engagement and client satisfaction. We also put a lot of energy into explaining why banning the use of text and other off-channel communications was often ineffective.

Today, most of the global population own a smartphone and use it as their primary means of communication. The CTIA (Cellular Telephone Industry Association) estimated that in 2023, over 90% of the US population own a smartphone, and 15% use it exclusively to access the internet, with 2.1 trillion SMS and MMS exchanged. In June 2024, Meta Platforms estimated that WhatsApp users surpassed 3 billion. The GSMA (Global System for Mobile Communications Association) states that, in 2022, 2.6 billion people accessed financial information via their smartphones, and over 2 billion accessed government services with their mobile devices.

Regulatory requirements for mobile communication recordkeeping

Previously, we also invested significant time explaining the regulatory recordkeeping requirements for mobile communication channels (SMS/text, MMS, chat) and personal BYOD devices within the highly regulated financial services sector, and the potential negative impact violations might have if an organization was found noncompliant.

The Securities and Exchange Commission (SEC), Commodity Futures Trading Commission (CFTC), Financial Industry Regulatory Authority (FINRA), Financial Conduct Authority (FCA), the Office of Gas and Electricity Markets (OFGEM), and other global regulators have made this clear in their guidance.

As you begin conducting due diligence on any third-party technology partner, it is essential that their information security strategy, policies and culture value confidentiality, integrity and availability

Over 2 billion people worldwide accessed government services with their mobile devices in 2022

Source: GSMA

In the USA, for example, the Exchange Act Rules 17a-3 and 17a-4, as well as FINRA Rule 3110(b)(4) (Review of Correspondence and Internal Communications) and FINRA Rule Series 4510 (Books and Records Requirements) require a firm to, among other things, create and preserve, in an easily accessible place, originals of all communications received and sent relating to its "business as such." If a firm permits its associated persons to use a particular application—for example, an app-based messaging service or a collaboration platform—the firm must preserve records of business-related communications and supervise the activities and communications of those persons on the application. Firms remain responsible for conducting due diligence to comply with the securities laws and FINRA rules and follow up on red flags of potentially violative activity. In some cases, they may use services provided by the relevant digital channel or third party vendors.

Over $3 billion in financial penalties so far in global recordkeeping and supervision violations sweep

The highly publicized global recordkeeping and supervision violation sweep began in December 2021, with a major US financial institution paying $200 million to the SEC and CFTC because employees often communicated about securities business matters on their personal devices, using text messages, WhatsApp, and personal email accounts. The firm did not preserve these records as required by the federal securities laws.

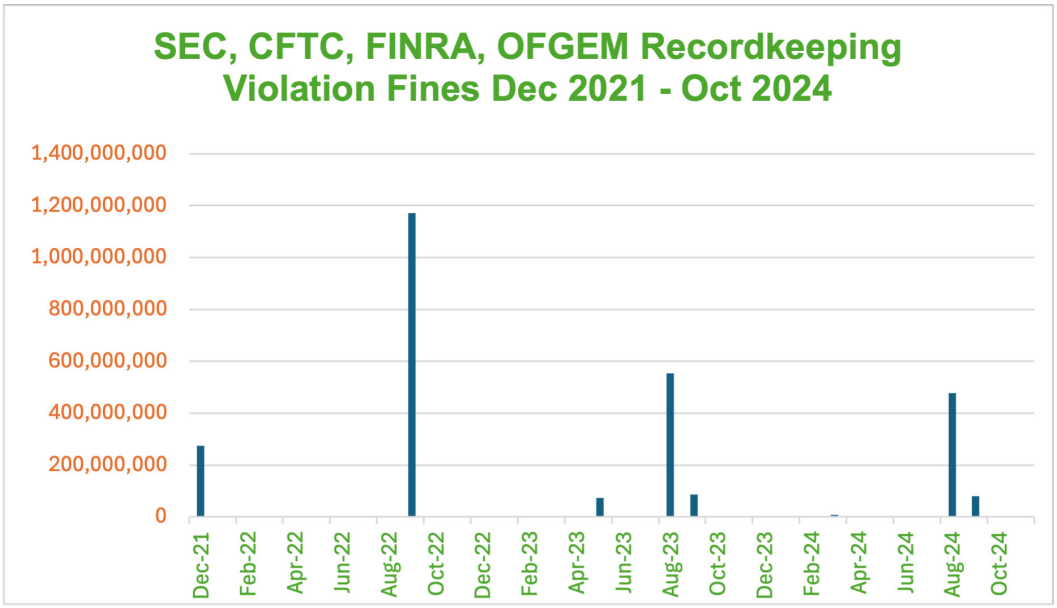
In September 2022, sixteen Wall Street firms admitted wrongdoing and agreed to pay more than $1.1 billion in penalties for widespread and longstanding failures by the firms and their employees to maintain and preserve electronic communications. They acknowledged that their conduct violated recordkeeping provisions of the federal securities laws.

In May 2023, the SEC continued with its sweep by charging two large financial institutions with violating recordkeeping provisions of the federal securities laws. Both agreed to pay penalties of $15 million and $7.5 million, respectively.

A few months later, in August 2023, the next round of investigations and fines were levied, with the SEC charging eleven Wall Street firms with penalties totalling $289 million.

Over 90% of the US population owned a smartphone and exchanged 2.1 trillion SMS and MMS in 2023

Source: CTIA



Enterprise level software should have seamless integration capabilities, offer customization options, built in analytics and provide easy user administration and scalability

The following month, in September 2023, OFGEM levied the first-ever fine issued in the UK under legal requirements to record and retain electronic communications relating to trading wholesale energy products. The major global financial institution paid $6.8 million for communications made by wholesale energy traders, on privately owned phones via WhatsApp that discussed energy market transactions between January 2018 and March 2020.

The same month, the SEC announced charges against five broker-dealers, three dually registered broker-dealers and investment advisers, and two affiliated investment advisers for widespread and longstanding failures to maintain and preserve electronic communications. The firms agreed to pay combined penalties of $79 million.

Off-channel communications sweep showing no sign of abating

The recordkeeping and supervision investigations showed no signs of slowing down when, in early 2024, the Financial Industry Regulatory Authority (FINRA) began levying significant financial penalties and censures against several broker-dealer firms for the systematic use of unsupervised off-channel communications for business.

In August 2024, the SEC announced charges against 26 broker-dealers, investment advisers, and dually registered broker-dealers and investment advisers for widespread and longstanding failures by the firms and their personnel to maintain and preserve electronic communications who agreed to pay combined civil penalties of $392.75 million. Three of the firms self-reported their violations and, as a result, paid significantly lower civil penalties than they would have otherwise.

In September 2024, the SEC charged six nationally recognized statistical rating organizations (NRSRO) for significant failures by the firms and their personnel to maintain and preserve electronic communications. The organizations agreed to pay penalties totalling more than $49 million.

CellTrust is here to help you make SMS/ texting and mobile communication compliance possible within your organization

The SEC, CFTC, FINRA, FCA, OFGEM, and other global regulators have definitive record-keeping compliance guidance

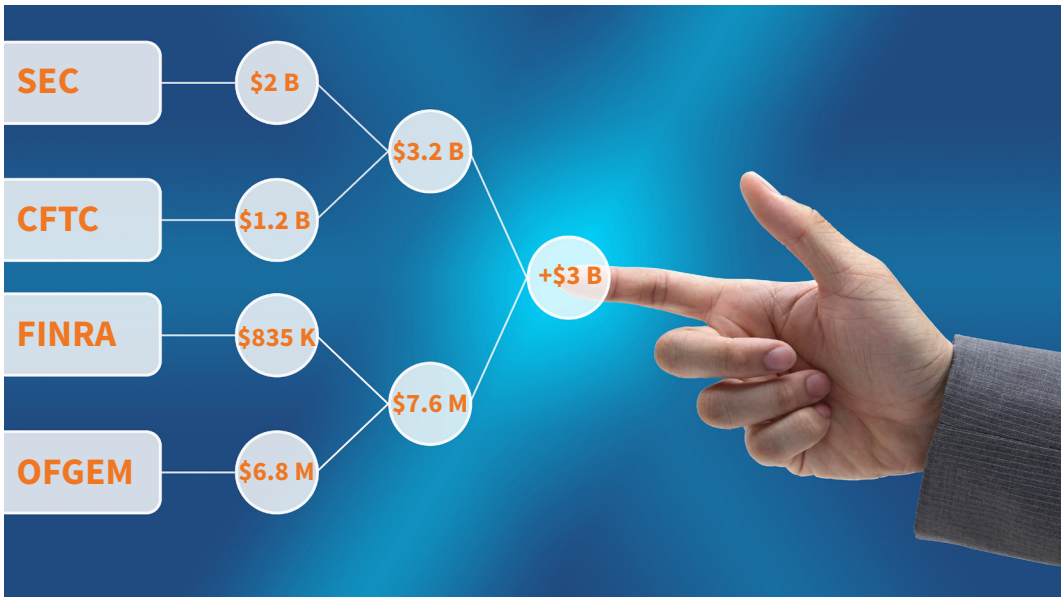
The same month, the SEC charged twelve municipal advisors with failures by the firms and their personnel to maintain and preserve certain electronic communications. The firms agreed to pay more than $1.3 million combined civil penalties to settle the SEC's charges.

One week later, the SEC announced charges against twelve firms, comprising broker-dealers, investment advisers, and one dually registered broker-dealer and investment adviser, for widespread and longstanding failures by the firms and their personnel to maintain and preserve electronic communications in violation of recordkeeping provisions of the federal securities laws. The firms agreed to pay combined civil penalties of $88,225,000, were ordered to cease and desist from future violations of the relevant recordkeeping provisions and were censured. Ten of the firms also agreed to retain compliance consultants to, among other things, conduct comprehensive reviews of their policies and procedures relating to the retention of electronic communications found on personal devices and their respective frameworks for addressing non-compliance by their personnel with those policies and procedures.

From December 2021 to September 2024, the CFTC imposed over $1.2 billion in civil monetary penalties on 27 financial institutions for using unapproved methods of communication in violation of CFTC recordkeeping and supervision requirements.

As of this publication date in November 2024, the total financial penalties levied by the global regulators mentioned previously for off-channel communication recordkeeping violations total over $3 billion.

As a long standing Microsoft Cloud Partner and member of the Microsoft Intelligent Security Association, the CellTrust SL2 platform is engineered in the Azure Cloud



There have been over $3 billion in financial penalties in global recordkeeping and supervision violations sweep since December 2021

Failure to capture and preserve off-channel communications

In SEC press releases relating to the off-channel violations, they state that the investigations uncovered pervasive and longstanding off-channel communications at all the firms. The SEC discovered that employees often communicated on their personal mobile devices through various messaging platforms about business related matters.

Furthermore, the firms did not maintain or preserve the substantial majority of these off-channel communications. By failing to maintain and preserve these off-channel communications on personal devices, the firms violated US federal securities laws and likely deprived the SEC and CFTC of these off-channel communications in various investigations. The failures involved employees at multiple levels of authority, including supervisors and senior executives.

When will the FCA crackdown on off-channel communications?

As of October 2024, the Financial Conduct Authority (FCA) in the UK, has been having discussions with UK financial institutions regarding nonmonitored off-channel communications on noncompany platforms. Thus far, they have not announced an official probe across the UK financial sector, however, some industry thought leaders believe it is only a matter of time.

What to look for in an enterprise grade secure and compliant mobile business communications solution

In today's complex, rapidly changing IT environment, businesses need a trusted partner who stays on top of developing technologies and device capabilities and understands how leading with a mobile-first strategy can result in significant enterprise gains.

BYOD, CYOD, COPE or COBO , CellTrust's mobility solutions can empower your enterprise

Scrutiny is continuously being heightened by regulators around the world to protect customer data and this is particularly the case within the financial services sector

Founded by leaders in internet and mobile security, and driven by a team passionate about empowering a mobile world, CellTrust is here to support you through planning, integration, implementation, and execution, resulting in a seamless, secure and compliant mobile business communications solution.

Founded by security pioneers - a team at the leading edge

CellTrust co-founders Sean and Kevin Moshir, cybersecurity authorities for over 30 years, have advanced expertise in information security strategy for enterprises and government. They are pioneers of anti-virus and the multibillion-dollar enterprise patch management industry and patent inventors for over 60 US and international patents addressing mobile security and compliance.

Member of the Microsoft Intelligent Security Association (MISA)

CellTrust is also a member of the Microsoft Intelligent Security Association (MISA), consisting of Microsoft premier security partners—independent software vendors (ISVs) and managed security service providers (MSSPs) that have integrated their solutions with Microsoft Security products. The approximate 400 MISA members (nominated by Microsoft) are experts from across the cybersecurity industry and have the shared goal of improving customer security.

SEC Regulation S-K Item 106 asks for a description of cybersecurity processes and clarification of the processes to oversee and identify material risks from cybersecurity threats associated with using any third party service provider

SL2 Enterprise Capture is packed with easy to use, compliance related messaging features to reduce the risk of violations

A technology partner with a profound understanding of cybersecurity and the threat landscape

It's been culminating for years, and with the latest release in June 2024 of the recent SEC Cybersecurity Compliance and Disclosure Interpretations (C&DIs), regulated entities should be in no doubt that the responsibility for cybersecurity lies firmly in the boardroom.

The SEC now requires market entities to implement policies and procedures reasonably designed to address cybersecurity risks and review and assess their design and effectiveness at least annually.

Regulation S-K Item 106 asks for a description of cybersecurity processes and how they have been integrated into the entity's risk management system. Further, they must disclose the use of assessors, consultants, auditors, or other third parties concerning cybersecurity processes. They must also clarify the processes to oversee and identify material risks from cybersecurity threats associated with using any third party service provider.

Additionally, entities are required to clarify whether any risks from cybersecurity threats, including any derived from a previous cybersecurity incident, have materially affected or could reasonably materially affect the entity's business operations, strategy, or finances and, if so, how. The SEC requires firms to disclose and report on material cybersecurity incidents within four days.

Increased attacks on third party technology providers

In September 2024, FINRA issued guidance on cybersecurity advisory third party provider risks. The organization observed a significant increase in the number of cybersecurity incidents experienced by third party providers used by FINRA member firms. Upon review, it determined that vulnerabilities in legitimate system management tools and technology products used by third party providers were targeted.

In 2024, FINRA has observed a significant increase in the number of cybersecurity incidents experienced by third party providers used by FINRA member firms

Along with more than 95 percent of Fortune 500 companies and small and large businesses worldwide, CellTrust leverages the multilayered security provided by Microsoft across physical data centers, infrastructure, and operations in Azure

The 2024 threat landscape across third party provider platforms included data breaches with ransomware, resulting in leaked customer data, and Zero Day vulnerabilities that exploited access to company data before patching could occur.

Several Zero Day attacks resulted in full-blown extortion and ransom events, and ultimately, the exposure of firm and customer data and the threat of possible follow-on identity theft of individuals.

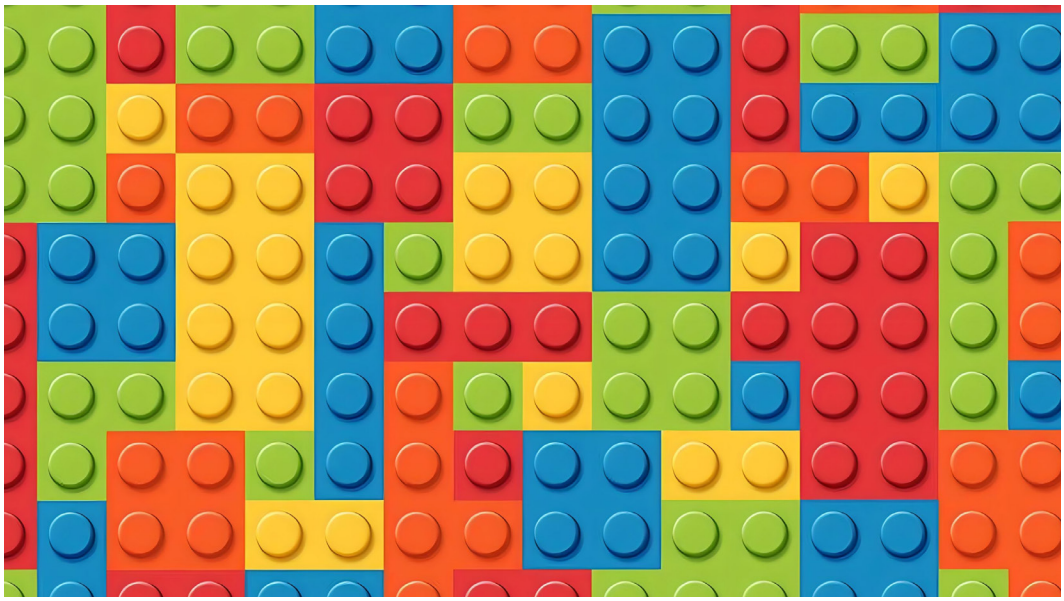
Further, weather-related outages were exploited through social engineering and third party provider impersonation campaigns. Threat actors impersonating a third party provider claimed they would correct the outage with a fix but instead loaded malware onto computers to steal credentials.

Cybersecurity due diligence and accountability

In addition to the SEC and FINRA - the FCA, Markets in Financial Instruments Directive (MiFID II), EU General Data Protection Regulation (GDPR), US Department of the Treasury, US Federal Trade Commission (FTC), and other federal and state regulators are scrutinizing financial services firms to ensure that they are practicing cybersecurity due diligence on any third party technology partners while making sure they have cybersecurity leadership, strategy, policies and processes in place to protect customers and markets.

Should a security breach be caused by a third party technology provider's vulnerability or lack of cybersecurity best practices, the provider will undoubtedly be held accountable. However, the financial services entity will ultimately bear the brunt of the potential financial loss, violations, penalties, and reputation and brand damage for lack of cybersecurity due diligence and any potential cybersecurity mismanagement.

SL2 Enterprise Capture Is integrated with the leading UEM/ EMM solutions: Microsoft Intune, Ivanti Neurons™, BlackBerry® Dynamics™ and AppConfig



Several Zero Day attacks resulted in full-blown extortion and ransom events, and ultimately, the exposure of firm and customer data and the threat of possible follow-on identity theft of individuals

Verifying the cybersecurity readiness of your third-party technology partner

As you begin conducting due diligence on any third-party technology partner, it is essential that their information security strategy, policies and culture value confidentiality, integrity and availability.

"While cybersecurity best practices are continually evolving, third-party technology providers for the financial services sector must be ready to effectively adopt the latest industry standards to stay current and be able to provide meaningful responses to the customers' due diligence requests for vendor risk management." – Kevin Moshir, CellTrust Co-founder and COO

CellTrust stays up to date with multiple cybersecurity frameworks including, the National Institute of Standards and Technology (NIST) and NIST SP 800-53, which influence our security posture and annual review:

- NIST SP 800-53 includes controls for the development of secure and resilient information systems, providing operational, technical, and management standards and guidelines that information systems should use to maintain confidentiality, integrity, and availability.
- The standards and guidelines from NIST incorporate a multi-tiered approach to risk management through these controls.
- The controls are set forth in three classes indicating impact: low, moderate, and high.

UEM enables a rich set of mobile application protection policies to safeguard client data and protect enterprises against cyber attacks while providing employees with seamless access to corporate apps and data

CellTrust's customers range from one person Registered Investment Advisors to mid-sized broker-dealer entities, large financial services organizations to some of the world's largest global wealth management and banking institutions

Incident response and breach notification

As required by cybersecurity best practices and many international, federal, state, and local laws, should a breach occur, CellTrust immediately stands up a dedicated CellTrust Incident Response Team and notifies the customer. The CellTrust Incident Response Team will then support the customer and their stakeholders, including insurance agencies and the relevant international, federal, state, and local government agencies governing the specific breach.

What defines an effective compliance program?

The DOJ has also identified five key factors in a security compliance program they consider when evaluating its effectiveness, and those can be addressed with the following action items:

- Have a qualified third party conduct an annual risk analysis/risk assessment.
- Perform a review of all policies and procedures at least annually to ensure they are comprehensive and up to date.
- Ensure that the workforce undergoes ongoing and appropriate training.
- Ensure that effective reporting structure and investigation process is in place and communicated to the workforce.
- Implement appropriate agreements with and ongoing monitoring of third parties to protect privacy and security.

For a security compliance program to effectively engage third parties, those agreements should address three key areas:

- Confirm that appropriate technical, administrative, and physical safeguards have been implemented.
- Ensure there are explicit requirements for breach notification.
- Ensure that data disposal/return occurs when the relationship ends.

When finding the right third party technology partner to meet your organization's mobile communication compliance requirements, there are additional cybersecurity considerations to put on your checklist

The Azure global infrastructure serves more than any other cloud provider across 60+ regions. With more than 68,000 partners, the Microsoft Azure partner network is broad and experienced, with more compliance certifications than others in the industry

CellTrust adheres to the SEC and DOJ compliance hallmarks and five security to-dos with continuous review, testing and improvement of its cyber, information and data security processes.

CellTrust is audited annually by a qualified, nationally recognized **American Institute of Certified Public Accountants (AICPA) System and Organization Controls (SOC)** third party auditor. All staff receive Risk Management Training upon hire and annually with a focus on cyber, information and data security best practice. Security and privacy agreements are in place with all CellTrust SL2 vendors that address the three key areas above and current state and country privacy law requirements applicable to CellTrust's customers.

Mobile communications compliance cybersecurity checklist

Enterprise mobile users may access the network from anywhere, so Administrators are challenged to balance productivity needs with security requirements.

Enterprise grade secure mobile communication and messaging platforms, unlike consumer grade apps, are engineered and constantly monitored with data loss prevention and cyber defense in mind. While consumer grade solutions may provide some security features such as encryption, a form of multilevel authentication, and remote wipe, they often need more robust security rules, policies, and processes an enterprise-grade solution has been engineered with.

It is also essential for mobile communication and messaging applications to be stored in a Secure Cloud Computing Architecture (SCCA) certified cloud environment where encryption key management lifecycle services with optional dedicated hardware security modules and transparent data encryption for encryption at rest are standard. Best practices for all cryptography operations, including strong encryption for all data in motion and transmission across the internet, must also be applied.

SL2 Enterprise Capture is archiving agnostic — with multiple Enterprise Information Archiving (EIA) options available for text, MMS, chat, voice, separate voice and SMS endpoints, and short code

SL2 Enterprise Capture is flexible, scalable and affordable and can be customized to meet the specific capture and compliance needs of the financial services firm within a specific budget

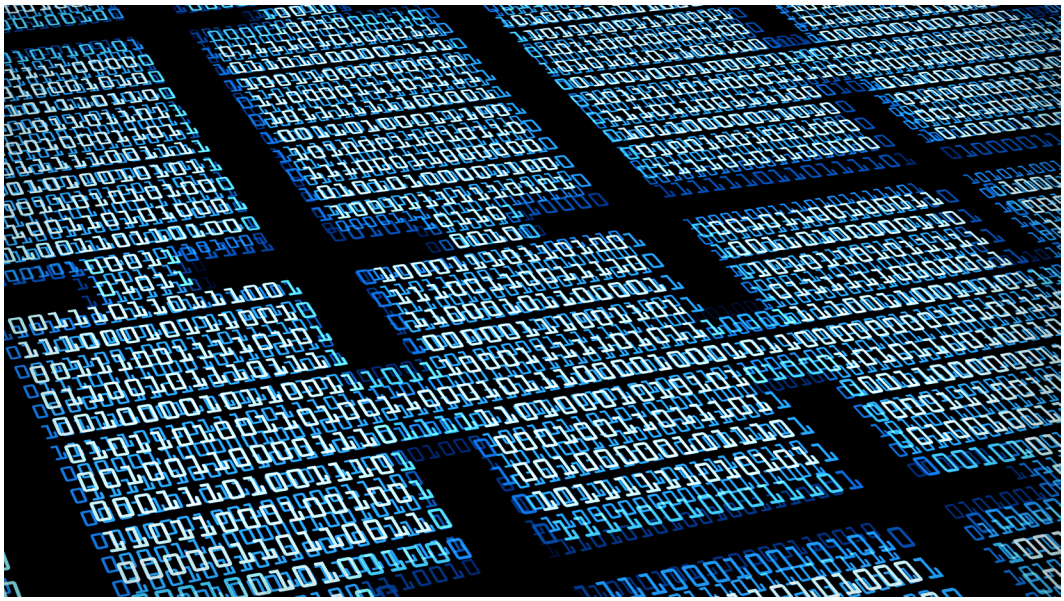
Zero Trust architecture is a best practice designed to protect by leveraging network segmentation, preventing lateral movement, providing layered threat prevention, and simplifying granular user-access control. The foundational building block for the Zero Trust network model is Active Directory (AD), which vastly enhances network security and safeguards access to enterprise data through identity management and conditional access control for both devices and users.

"It is important to understand that, while related, there is a difference between cybersecurity and privacy. Cybersecurity protects information and systems, and, while you can have security without privacy, privacy is NOT feasible without security. There is no way to keep data private and personal without proper security protections." – Rebecca Ruegg-Lerner, CellTrust General Counsel

Robust data protection and privacy

Scrutiny is continuously being heightened by regulators around the world to protect customer data and this is particularly the case within the financial services sector.

CellTrust is an industry leader trusted by three of the top ten US banks and have tens of thousands of dedicated users worldwide



In September 2024, FINRA issued guidance on cybersecurity advisory third party provider risks. The organization observed a significant increase in the number of cybersecurity incidents experienced by third party providers used by FINRA member firms

The SEC, CFTC, FINRA, FCA, EU GDPR, MiFID II, and many other regulatory bodies around the world are requiring financial firms to take significant steps to ensure text messages and other mobile communications are stored securely in a tamper-proof environment. As well, these communications must be readily available and searchable for eDiscovery audits and investigations.

What is "Data Minimization?"

CellTrust limits the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which the personal data is processed, as disclosed in the privacy notice. This is recognized as the practice of data minimization.

Privacy and security by design

Privacy and security are Integral to organizational priorities, project objectives, design processes, and planning at CellTrust and include these actions:

- Being proactive instead of reactive.
- Identifying risks and mitigating those risks or determining if you can accept some risks.
- Taking a multidisciplinary design approach across the organization from the start.
- Remaining at the forefront of security and privacy regulations and developments.

In 2022, 2.6 billion people accessed financial information via their smartphones

Source: GSMA

CellTrust stays up to date with multiple cybersecurity frameworks including, the National Institute of Standards and Technology (NIST) and NIST SP 800-53, which influence our security posture and annual review

Protecting consumers' nonpublic personal information (NPI) held by financial institutions

The Gramm Leach Bliley ACT (GLBA) stipulates privacy requirements focused on protecting consumers' nonpublic personal information (NPI) held by financial institutions. GLBA has several requirements regarding data protection.

GLBA provisions can be enforced by CFPD, FDIC, Consumer Financial Protection Bureau, FTC, and other regulators. Certain data is subject to carve outs at the state level.

Here's a breakdown of the key points:

- NPI Definition: (i) Personally identifiable financial information; and (ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.
- Transparency: Financial institutions must provide customers a clear and conspicuous privacy notice that details what information is collected, how it's used, and with whom it's shared.
- Opt-Out Right: With some exceptions, such as for servicing accounts or fraud prevention, customers must have the right to opt-out of having their NPI shared with nonaffiliated third parties for marketing purposes.

CellTrust adheres to the SEC and DOJ compliance hallmarks and five security key factors with continuous review, testing and improvement of its cyber, information and data security processes

Will AI heighten the threat of global ransomware?

The British National Cyber Security Centre (NCSC) suggests it will. In a recent report the NCSC made the assessment that AI will almost certainly increase the volume and heighten the impact of cyberattacks over the next two years. They state they are already seeing cybercriminals of all trades using AI in the initial stages of attacks to increase their effectiveness.

The SEC now requires market entities to implement policies and procedures reasonably designed to address cybersecurity risks and review and assess their design and effectiveness at least annually

"All types of cyber threat actor – state and non-state, skilled and less skilled – are already using AI, to varying degrees." – British National Cyber Security Centre (NCSC)

The impact is expected to grow for several reasons:

- AI can be utilized to improve existing tactics, techniques, and procedures.
- AI can assist with reconnaissance and social engineering to help target victims.
- AI can assist in analyzing stolen data can be analyzed for even more effective attacks.
- Cybercriminals are able to compose more effective phishing emails with the help of AI.
- Convincing interaction with victims can be incorporated with the use Generative AI (GenAI), including the creation of lure documents that will lack the errors (like in translation, spelling, and grammar) that used to be clear indicators of phishing.
- State sponsored attackers and other more advanced threat actors are apt to be on the forefront of more sophisticated methods to utilize AI and others will follow.

CellTrust does not use Generative AI in its products or platform

Artificial Intelligence, or AI: the mere mention of the phrase can increase the heart rate of compliancy professionals as they contemplate the implications of this evolving technology and the impacts it can have on privacy, confidentiality, and intellectual property (IP). However, it is essential to understand an important distinction between AI, Generative AI (GEN AI), and Artificial General Intelligence (AGI) when evaluating technologies in order to better understand the true level of risk involved. AGI occurs when a technology system can operate intellectually similar to a human, and GEN AI involves learning patterns and content creation by technology. Traditional AI is limited to analyzing existing data with no machine learning or content

SL2 Enterprise Capture communications are encrypted in transit and at rest while in CellTrust's network

Enterprise grade secure mobile communication and messaging platforms, unlike consumer grade apps, are engineered and constantly monitored with data loss prevention and cyber defense in mind

generation. This means that traditional AI only uses the information it was programmed to use in order to make an analysis and perform designed operations.

CellTrust's SL2 offering in its standard form, does not use any type of AI. CellTrust does offer its customers an optional Content Moderator feature that utilizes traditional AI (not GEN AI nor AGI), and this tool does not include learning patterns or anything near the human thought process. Instead, during set up, the customer's assigned SL2 administrator provides the information to the Content Moderator that it wants the moderator to utilize in performing its analysis. The Content Moderator learns nothing from the messages it reviews to determine if the criteria set by the SL2 administrator were met. The only way that the Content Moderator's criteria for analysis will change is if the SL2 Administrator manually changes the criteria in the setup.

CellTrust's use of traditional AI (not GEN AI nor AGI), means the Content Moderator is not gaining information from the messages it reviews and cannot use the content of those messages, or details about who is sending or receiving the messages, for any purpose except to report if a message meets the criteria established by the SL2 Admin, which greatly restricts the risks to privacy, confidentiality, and IP when used.

Engineered in the Azure Cloud

As a long standing Microsoft Cloud Partner and member of the Microsoft Intelligent Security Association, the CellTrust SL2 platform is engineered in the Azure Cloud utilizing world class application development and leading edge security. The Azure cloud is built with customized hardware, has security controls integrated into the hardware and firmware components, and added protections against threats such as DDoS. Benefit from a team of more than 3,500 global cybersecurity experts who work together to help safeguard your business assets and data in Azure.

CellTrust limits the collection of personal data to what is adequate, relevant, and reasonably necessary

CellTrust leverages the multilayered security provided by Microsoft across physical data centers, infrastructure, and operations in Azure, along with more than 95 percent of Fortune 500 companies and small and large businesses worldwide. The Azure global infrastructure serves more than any other cloud provider across 60+ regions. With more than 68,000 partners, the Microsoft Azure partner network is broad and experienced, with more compliance certifications than others in the industry.

Available within the Azure Government Cloud

SL2 Enterprise Capture is also available as a dedicated instance within the Azure Government Cloud, which offers the broadest level of certifications of any cloud provider to simplify even the most critical government compliance requirements, such as FedRAMP, NIST 800.171 (DIB), ITAR, IRS 1075, DoD L4, and CJIS.

Source: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-azure/

Engineered at enterprise level

SL2 Enterprise Capture is enterprise level software. This means it is engineered to protect the enterprise from cyber attacks or data loss while enhancing productivity and efficiency for organizations of all sizes - some with mission critical operations. At the same time, it should have seamless integration capabilities, offer customization options, built in analytics and provide easy user administration and scalability to support organizational growth.

Artificial Intelligence, or AI: the mere mention of the phrase can increase the heart rate of compliancy professionals as they contemplate the implications of this evolving technology and the impacts it can have on privacy, confidentiality, and intellectual property (IP)

CellTrust's SL2 offering in its standard form, does not use any type of AI. CellTrust does offer its customers an optional Content Moderator feature that utilizes traditional AI (not GEN AI nor AGI), and this tool does not include learning patterns or anything near the human thought process

BYOD, CYOD, COPE or COBO

CellTrust's experienced team can demonstrate how our market-leading mobility solutions can empower your enterprise with secure, compliant bring your own device (BYOD), choose your own device (CYOD), corporate owned personally enabled device (COPE), and corporate owned business enabled device (COBO) mobile communications. They can also work with you to determine which approach, or if a blended approach, will help you meet your organization's mobile productivity and compliance aspirations.

Integrated with the leading UEM/EMMs

CellTrust SL2 Enterprise Capture is one of the few, if not the only, compliant mobile text capture applications available on four leading Unified Endpoint Management (UEM) and Enterprise Mobility Management (EMM) solutions.

CellTrust collaborates with the UEM/EMM market leaders to provide mobile device, app, and content management for BYOD, CYOD, COPE and COBO environments.

UEM solutions provide a single user endpoint management platform for all device types across the mobile enterprise ecosystem, simplifying device management and configuration. With single-sign-on, conditional access, mobile threat defense and AI insights, UEM enables a rich set of mobile application protection policies to safeguard client data and protect enterprises against cyber attacks while providing employees with seamless access to corporate apps and data.

CellTrust customers can select from a range of secure UEM and EMM solutions integrated with SL2 Enterprise Capture which provide leading edge mobile device management, mobile app management and mobile content management: Microsoft Intune, Ivanti Neurons™, BlackBerry® Dynamics™ and AppConfig.

Capturing the leading communication channels

SL2 Enterprise Capture is integrated with many of the most popular collaboration apps so that employees can connect with customers on the channels they prefer and commonly use.

Rich in features, collaborative and easy to use

Developed with compliance in mind, SL2 Enterprise Capture is packed with easy to use, compliance related messaging features to ensure your team and organization can reduce the risk of violations. Compliant SMS/MMS and Group MMS, private chats, group chats, scheduled messages, and broadcast announcements/bulletins and chats are enabled. Messaging templates, personal signatures and corporate disclaimers are provided and can easily be customized and updated. Search message body, phone number blocking and automatic replies are also valued features.

SL2 Enterprise Capture is enterprise level software. This means it is engineered to protect the enterprise from cyber attacks or data loss while enhancing productivity and efficiency for organizations of all sizes - some with mission critical operations

SL2 Enterprise Capture is integrated with many of the most popular collaboration apps so that employees can connect with customers on the channels they prefer and commonly use

Scalable and budget competitive

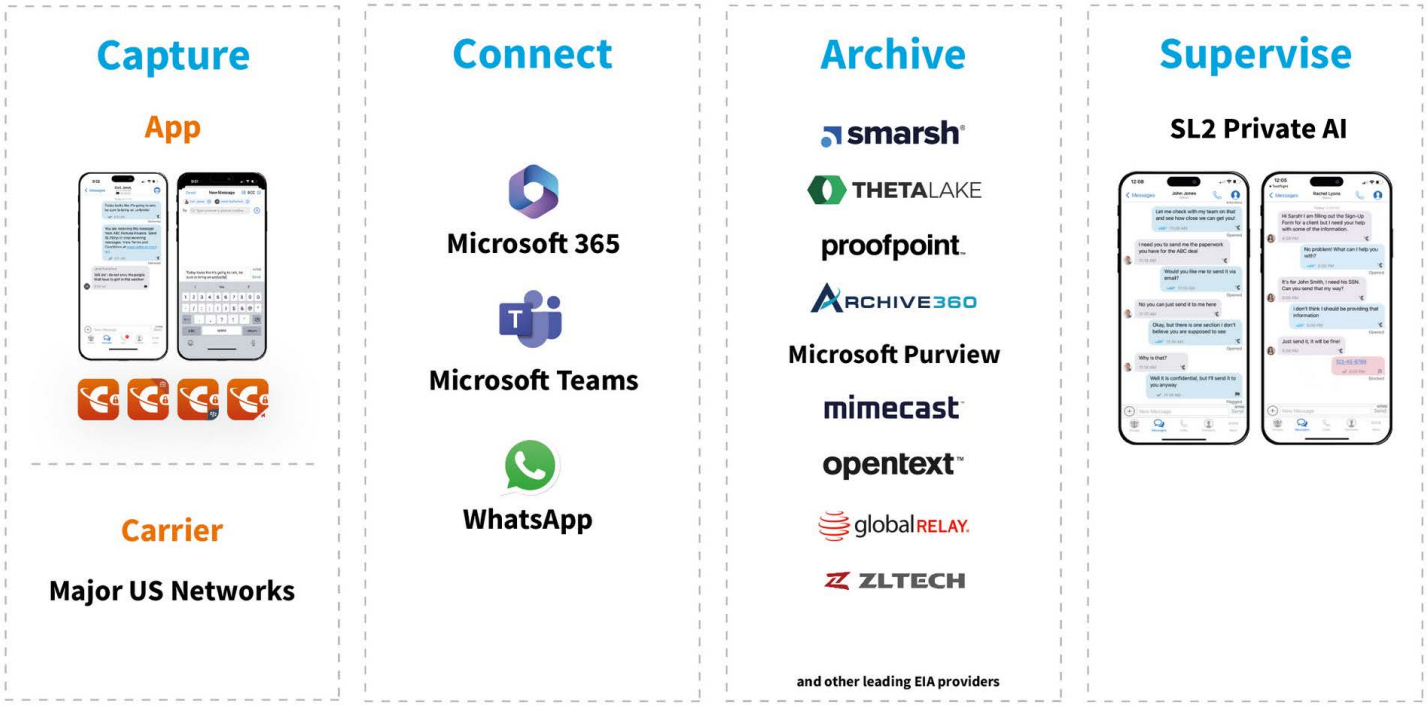
CellTrust's customers range from one person Registered Investment Advisors to mid-sized broker-dealer entities, large financial services organizations to some of the world's largest global wealth management and banking institutions.

SL2 Enterprise Capture is flexible, scalable and affordable and can be customized to meet the specific capture and compliance needs of the financial services firm within a specific budget.

Agnostic - yet integrated with the leading EIAs

SL2 Enterprise Capture is archiving agnostic — with multiple Enterprise Information Archiving (EIA) options available for text, MMS, chat, voice, separate voice and SMS endpoints, and short code.

CellTrust customers can choose to have a custom archiving solution, bring their organization's current archiving platform with them, or select from one of CellTrust's leading EIA technology partners:



Dedicated implementation team

A dedicated CellTrust project manager will ensure your rollout is as seamless as possible. Live training will maximize user adoption. Continuously updated user guides and videos serve as a quick reference, and CellTrust's friendly Customer Support team is also here to help.

Recommended by compliance and IT professionals

https://www.celltrust.com/company/customers/

https://www.celltrust.com/resources/case-studies/

https://customers.microsoft.com/en-us/story/1503067502270490175-visionary-wealth-advisors-banking-capital-markets-microsoft-security-solutions

Trusted and proven with tens of thousands of users around the world

CellTrust is here to help you make SMS/texting and mobile communication compliance possible within your organization. It begins with our Solution Engineers delivering a seamless planning, integration, implementation and execution experience. That's why we are the industry leader trusted by three of the top ten US banks and have tens of thousands of dedicated users worldwide.

Helpful links:

https://www.sec.gov/newsroom/press-releases/2023-52

https://www.sec.gov/newsroom/press-releases/2023-139

https://www.finra.org/rules-guidance/guidance/cybersecurity-advisory-third-party-provider-risks

https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat

https://www.celltrust.com/secure-sms-mms-patent-awarded-celltrust/

https://www.celltrust.com/celltrust-sms-archiving-technology-patent-awarded/

https://www.celltrust.com/celltrust-nominated-microsoft-become-member-microsoft-intelligent-security-association-misa/

https://www.celltrust.com/resources/patents-rights/

Industry Recognition:

Member of
Microsoft Intelligent Security Association

Microsoft Security

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations ™

MOBILE BREAKTHROUGH AWARD 2024
MOBILE COMPLIANCE PLATFORM OF THE YEAR

Get it from Microsoft Azure Marketplace

Learn more

Talk with an expert. Book a 15 minute introductory call with a CellTrust Solutions Engineer.

Reach out so that our experienced team can help you balance security, compliance and productivity with secure, compliant, enterprise level mobile communication. Let's get started!

+1-480-515-5200, sales@celltrust.com or **www.celltrust.com/SL2**

HEADQUARTERS
20701 N. Scottsdale Rd.
Suite #107-451
Scottsdale, AZ 85255 USA
+1-480-515-5200

CANADA
1500 West Georgia, 13th Floor
Vancouver V6G 2Z6
+1-778-375-3236